A Novel Characterization Approach for Hand Geometry-Based Verification

Prof. Dr. Hilal Mohammed Yousof
Al-Rafidain U.C.
Baghdad – Iraq

Majid A. S. Sha'alan
Computer Sc. Dep.
Al-Mansour U. C.
Baghdad-Iraq

ABSTRACT

The objective of this paper is to investigate a novel biometric method based on hand geometry recognition for automatically verifying the identity of a person. Hand recognition is as a promising biometric which is being used in low-level security applications for several years. Unlike other hand geometry based systems, neither the user have to undergo the inconvenience of using pegs, nor the using of expensive dedicated capturing devices are employed. Hand features are extracted and used to generate some geometrical parameters that can be used to decide if two images belong to the same hand. Tests are conducted on image data sets taken from 50 users and the experimental results demonstrate that a FAR of 2% while maintaining a FRR of less than 3%, can be achieved by our method.

Introduction

As human interaction with networked society has become our daily addiction, the demand for reliable user authentication technologies has become more and more important. Traditional means of authentication require remembering lots of passwords, PINs, card keys, and other forgettable security codes. However, stronger authentication technologies, capable of providing higher degrees of certainty that a user is who he claims to be, are becoming commonplace. Biometrics is one of such strong authentication technologies.

Biometric technologies as we know them today have been made possible by the explosive advances in computing power and have been made necessary by the near universal connectedness of computers around the world. The increased perception of data and information as near equivalents of currency, in conjunction with the opportunities for access provided by the Internet, a paradigm shift with significant repercussions for authentication. If data is currency, then server-based or local hard drives are our new vaults, and information-rich companies will be held responsible for their security. Because of this, passwords and PINs are nearing the end of their life cycle for many applications. The leading biometric technologies-including finger-scan, facial-scan, voicescan, hand-scan, iris-scan, signature-scan, retina-scan, keystroke-scan, and Automated Fingerprint Identification Systems (AFISs)-each have their strengths and weaknesses, and are each well-suited for particular applications [1]. There is no single best biometric technology, nor is it likely that any single technology will come to dominate in every area of the biometric industry. Instead, the requirements of a specific application determine which, if any, is the best biometric [2]. While comparing the capabilities of finger-scan, facial-scan, and other leading technologies as a solution for a specific application-such as desktop one to one verification is very valuable, attempting to compare biometric technologies without an application is largely meaningless [1, 2, 3]. Hand recognition technology utilizes the distinctive aspects of the hand (in particular; the height and width of the palm and the fingers) to verify the identity of individuals. Hand recognition has been used for years in thousands of verification deployments. Hand-scan is a more application-specific solution than most biometric technologies, used exclusively for physical access and time and attendance applications. Hand recognition's strengths include that it is able to operate in challenging environments, it is an established, reliable core technology, and generally perceived as nonintrusive, which is based on a relatively stable physiological characteristic [4, 5, 6, 7, 8].

Previous work

In their development of an automatic personal identification system, Dapeng Zhang and Wei Shu have talked about what they did refer to by datum points in the palmprint as an invariant characteristics [9]. However, what they referred to; were the two endpoints obtained from the intersection of the principal lines with the sides of the hand. Their usage of these points was devoted to assess the right angle coordinate system that they used to handle the inconsistency of hand positioning. Slobodan Ribaric and his fellows [6], C. Poon and D. Wong [10], gave some cues about an approximation to two reference points located between the fingers, but they also used them only to define the focus-of-attention (FOAR) in their palmprint research. Wai King Kong and David Zhang [11] adopted a similar approach to extract the maximum region of interest in the palm.

Up to this point, neither of the above researchers, nor any other literatures have reported a practical methodology to extract and use the proposed feature points and use them directly for verification. It also seems worthily to report that A. Jain and Arun Ross [12], and Nicolae Duta [13] have separately developed verification systems that are based on the direct matching of the hand shapes. They used pegs to guide the hand to some consistent positioning in addition to the heavy computations needed in the point to point pairwise distance matching process they adopted.

In the proposed system, the data were collected using a document scanner. The users were let free to place their hands anywhere on the scanner. The only comment they were told was to keep their fingers normally little separated and the hand to be placed vertically as much as they could. The desktop of the scanner was set up not to let the thumb finger to be captured. This was done because of that the side view of its appearance provides no useful information for the processing.

Hand Image Acquisition

Hand features were extracted from the image of the right hand. There were no pegs, thus translation and rotation (about ± 20 related to the vertical line of symmetry of the scanner surface) was expected. A moderate resolution (about 200dpi) taken from 50 person (5 samples each) including: male and female, young and old people, workers, and others were adopted.

Preprocessing

To obtain hand images appropriate for feature extraction, the following steps were taken:

Step1: A trimming process is applied to get rid of the unuseful surrounding background followed by a translation transformation as a step toward obtaining a normalized version of the hand image.

Step2: A low pass filter is applied followed by a thresholding process to binarize the image.

Step3: A dilation process followed by erosion is applied to remove any small holes and to smooth out any interlacing anomalies in the hand region.

Step4: The boundary of the resulted image can be extracted using any edge detection routine, say Sobel.

Figure (1) illustrates the results of the above steps.

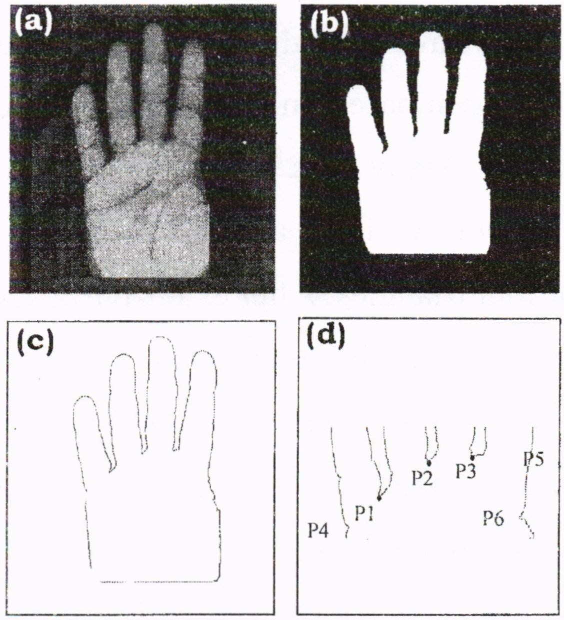

Figure (1): (a): Typical image obtained by a scanner, (b): the binarized image, (c): the image border, (d): the proposed feature points

Feature Extraction

The three holes located between each two adjacent fingers in the hand can be detected by segmenting the binarized image depending on some geometrical calculations into three sub-regions. The start and the end of each hole can be obtained by tracing the upper endpoints of the middle sub-region. The three points located on the head of each hole are extracted and used to find another three points as shown in Figure (1). Many possible triangular shapes can be held using the six points as vertices and connecting each three together. Eight of the possible triangles were chosen based on the possible unique features they might convey. Many tests were conducted to assess the stability and generality of this assumption and it was found to be valid for four triangles. After extensive observations, it was found that the line that the middle finger made when meeting the palm body, can be used to establish an appropriate hand coordinate system. The angle that is determined by this line with the horizontal line of symmetry of the hand image is used to rotate the image and obtain a completely normalized hand image. The adjusted feature points (after rotating the image) are extracted and used to calculate some other geometrical parameters to enhance the results. This biometric data is the feature vector.

Enrollment

In this process, the feature vectors (for each of the three training samples) is constructed and saved to the template file, In our proposed approach, the template file was too small (about 7 bytes only). The pertinent authentication information in which an authorized user is introduced to the system must be attached as well.

Verification

This one-to-one process is done by using the biometric information presented by the individual and those were already enrolled and saved under the same pertinent information. The two referenced template files are compared and the decision whether a match is to occur or not is performed by computing the length of each edge of the triangle using the Euclidean distance. Then, a theorem from elementary geometry is used to find out if the two triangles are similar on the basis of the overall rate between the corresponding edges of one triangle and their corresponding edges of the other. This operation is repeated for each of the other training samples. Then, a rated matching score taken from comparing the verification biometrics and each of the training biometrics is registered and found to produce more stable results. In addition to the traditional parameters of the evaluation criteria (FAR and FRR), a utilization of another important performance measure, namely TSR was used. Ying Han, Andrew T. B. J [14], introduced this measure.

Experimental Results

Table (1) summarizes (first row) the performance evaluation parameters of the system against a break-in attempt of one of the authorized users, and (second row) the same parameters for an outsider imposter attempt.

Table1: the performance evaluation parameters

Threshold	FAR	FRR	TSR
0.08	2%	3%	95%
0.11	2%	2.2%	95.8%

The average plots of false acceptance rate (FAR) and false reject rate (FRR) for different values of the threshold for the above attempts shows that while keeping FAR less than 2%, we can achieve FRR below 3% for the first and little greater than 2% for the second for verification, as illustrated in Figures (3) and (4).

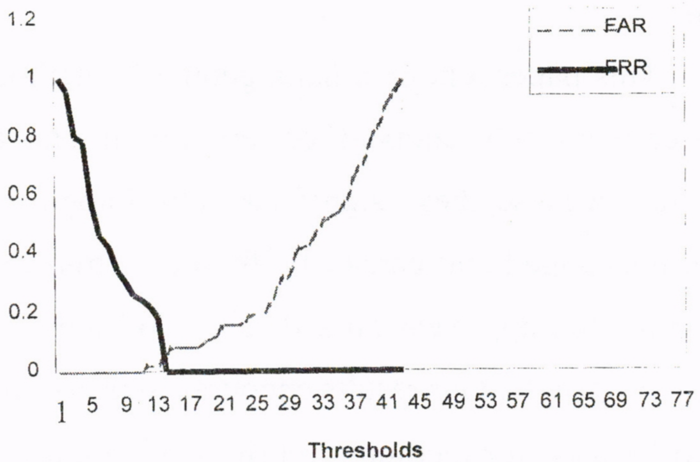

Figure (3): An illustration of the average plots of FAR and FRR of the system.

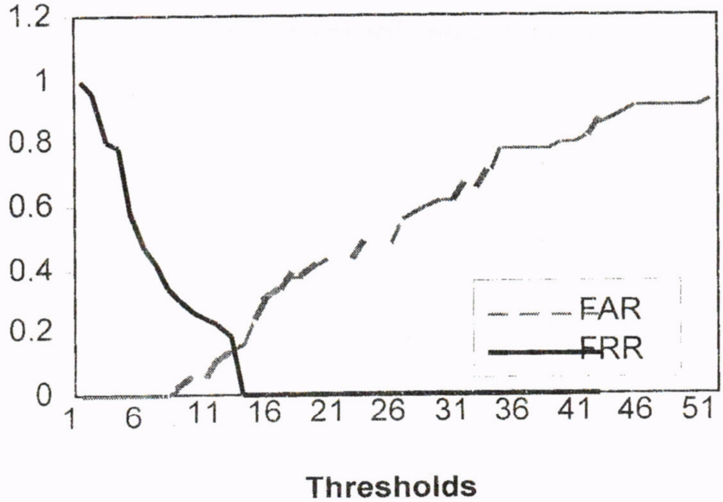

Figure (4): An illustration of the same parameters taken for an imposter attempt

Conclusion

This paper reports a hand geometry method using a new approach that can be adopted for verification. This approach is foolproofed because these significant physiological features are unique, unchanged and cannot be forged or transferred. We tested the proposed approach on a database of about 250 hand images from 50 people. Our results encouraged us to suggest this approach to be used for medium security applications. Stronger claims about the approach can be only made after conducting the experiments at a larger scale with samples collected over larger periods of time. Also, more investigations can be made to study the possible use of the system for identification.

References

[1] John Chirillo and Scott Blaul, " Implementing Biometric security," John Wiley Pub. Inc. 2003.

[2] Richard E. Smith, "Authentication From Passwords to Public Keys," Addison-Wesley 2002

[3] S. Nanavati, M. Thieme, and R. Nanavati," Biometrics: identity verification in a networked society," John Wiley and sons, Inc. 2002.

[4] Anil K. Jam, and Nicolse Dots. Deformable matching of hand shapes for verification. In Proceedings of International Conference on Image Processing, October 1999.

[5] Ajay Kumar, David C. M. Wong, "Personal Verification Using Palmprint and Hand Geometry Biometrics," AVBP, 2003, pp. 668-678.

[6] Yaroslav Bulatov, Sachin Jambwalikar, and others, "Hand Recognition Using Geometrical clsifiers,"

[7] Slobodan Ribric, Damir Ribaric, and Nikola Pavesic, "A Biometric Identification System Based on The Fusion of Hand Geometry and Palm Features,"

[8] Cenker Oden, Aytul Eril, Vedat Taylan Yildiz, Hikmet Kinnizitas, and Burak Buke. Hand recognition using implicit polynomials and geometric features. In Josef Bigin and Fabrizio Smeraldi, editors, Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication, volume 2091 of Lecture Notes in Computer Science, pages 336-341. Springer, June 2001.

[9] Dapeng Zhang and W. Shu, "Two novel characteristics in palmprint verification: datum point invariance and line feature marching," Pattern Recognition, vol. 32, no.4, pp. 691-702, 1999.

[10] C. Poon, D. C. M. Wong and H. C. Shen, "Personal Identification and Verification: Fusion of Palmprint Representation," carmenp, csdavid, helens @cs.ust.hk

[11] W. K. Kong and D. Zhang, "Palmprint texture analysis based on low-resolution images for personal authentication," Proc. ICPR-2002, Ouebec City (Canada).

[12] A.K. Jain, A. Ross, and S. Pankanti. A prototype hand geometry-based verification system. In Proceedings of 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication, pages 166—171, March 1999.

[13] N. Duta, A. K. lain, and Kanti V. Mardia, "Matching of Palmprint",
Pattern Recognition Letters, vol. 23, no. 4, Pp. 477-485, 2002.

[14] Ying Han, Andrew T. B. J, "Palmprint Verification with Moments," Journal of WSCG, Vol. 12, No. 1-3, ISSN 1213-6972.

طريقة مستحدثة للتمييز اعتمادا على الهيكل الهندسي لليد

أ. د. هلال محمد يوسف
كلية الرافدين الجامعة
بغداد – العراق

ماجد عبدالله سكر
كلية المنصور الجامعة
بغداد – العراق

المستخلص

الهدف من وراء هذه الورقة البحثية هو تطوير طريقة جديدة للتحقق من صلاحية مستخدم ما بواسطة تقنية التمييز المستندة الى الشكل الهندسي لليد hand geometry recognition وهي تقنية واعدة ومستخدمة بشكل فعال في المجالات ذات المستوى الأمني الغير عالي منذ مدة ليست بالقصيرة. الطريقة المقترحة تتصف بأنها لا تحتاج إلى استخدام أجهزة باهظة الثمن expensive dedicated capturing devices ولا إلى فرض سياقات يعاني منها المستخدم لاخذ عينات يد المستخدم كما هو متعارف عليه في الأنظمة المستخدمة حاليا. الطريقة تعتمد على استخراج بعض الخصائص المميزة التي يوفرها التركيب الهندسي ليد المستخدم ومن ثم إعمال برنامج مميز matcher لاعطاء القرار فيما إذا كانت عينة اليد تعود إلى شخص مخول بالاستخدام أم لا. التجارب أجريت على عينات أخذت من ٥٠ شخص وبواقع ٥ عينات لكل منهم (٣ منها خزنت كقاعدة بيانات والبقية استخدمت في اختبار المنظومة) أظهرت الاختبارات نتائج مشجعة (نسبة التمييز تراوحت ما بين ٩٥% و ٩٦%).