Using of Hand Geometry in Biometric Security Systems

Peter VARCHOL, Dušan LEVICKÝ

Dept. of Electronics and Multimedia Communications, Technical University of Košice,
Park Komenského 13, 041 20 Košice, Slovak Republic

Peter.Varchol@tuke.sk, Dusan.Levicky@tuke.sk

Abstract. *In this paper, biometric security system for access control based on hand geometry is presented. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Experiments show that the physical dimensions of a human hand contain information that is capable to verify the identity of an individual. The database created for our system consists of 408 hand images from 24 people of young ages and different sex. Different pattern recognition techniques have been tested to be used for verification. Achieved experimental results FAR=0,1812% and FRR=14,583% show the possibilities of using this system in environment with medium security level with full acceptance from all users.*

Keywords

Biometric security, hand geometry recognition, Gaussian mixture model, expectation-maximization algorithm.

1. Introduction

Associating an identity with an individual is called personal authentication. The person can be recognized by what he knows (e.g. password, PIN, or piece of personal information), by what he owns (e.g. card key, smart card, or token like a SecurID card) or by his human characteristics (biometrics). Biometric methods of person authentication belong in modern approaches in field of access security. The main advantage of biometric is that human characteristics cannot be misplaced or forgotten [1].

One of the most dangerous security threats is the impersonation, in which somebody claims to be somebody else. The security services that counter this threat are identification and verification. Identification is the service where an identity is assigned to a specific individual, and verification (authentication) the service designed to verify a user's identity.

Biometric methods can be generally divided into two categories:

- behavioral-based methods
- physiological-based methods.

Behavioral-based methods perform the authentication task by recognizing people’s behavioral patterns, such as signatures keyboard typing or voice print. The main problem with behavioral methods is that they all have high variations, which are difficult to cope with. On the other hand, while behavioral characteristics can be difficult to measure because of influences such as stress, fatigue, or illness, they are usually more acceptable to users and generally cost less to implement.

Physiological-based methods verify a person’s identity by means of his or her physiological characteristics such as fingerprint, iris pattern, palm geometry, DNA, or facial features. In general, traits used in the physiological category are more stable than methods in the behavioral category because most physiological features are virtually nonalterable without severe damage to the individual [3].

2. Hand Geometry

All biometric techniques differ according to security level, user acceptance, cost, performance, etc. One of the physiological characteristics for recognition is hand geometry, which is based on the fact that each human hand is unique. Finger length, width, thickness, curvatures and relative location of these features distinguish every human being from any other person. Hand geometry is considered to achieve medium security, but with several advantages compared to other techniques:

- medium cost as it only needs a platform and medium resolution reader or camera,
- it uses low-computational cost algorithm, which leads to fast results,
- low template size (from 352 to 1209 bytes), which reduces the storage needs,
- very easy and attractive to users – leading to great user acceptance,
- subconscious connection with police, justice, and criminal records.

The availability of low cost, high speed processors and solid state electronics made it possible to produce hand scanners at a cost that made them affordable in the commercial access control market. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The performance of these systems might be influenced if people wear big rings, have swollen fingers or no fingers. Although hand analysis is most acceptable, it was found that in some countries people do not like to place their palm where other people do. Sophisticated bone structure models of the authorized users may deceive the hand systems. Paralyzed people or people with Parkinson's disease will not be able to use this biometric method.

Since there is not much open literature addressing the research issues underlying hand geometry authentication, it is difficult to describe the state-of-the-art in using it in biometrics. Instead much of the available information is in the form of application-oriented description.

3. System Architecture

Typical architecture of all biometric systems consists of two phases:

- enrollment,
- recognition.

In the phase of enrollment, several images of hand are taken from the users. The images, called templates, are preprocessed to enter feature extraction, where a set of measurement is performed. Final model depends on the method used for recognition. Models for each of the users are then stored in the database. In the phase of recognition, a single picture is taken, preprocessed, and features are obtained. In the proposed system, the process of verification is used, where the input template is compared only with the model of claimed person. The feature vector is compared with features from the model previously stored in the database. The result is the person is either authorized or not authorized.

To evaluate a biometric system's accuracy the most commonly adopted metrics are the False Rejection Rate (FRR) and False Acceptance Rate (FAR). FRR is the percentage of authorized individuals rejected by the system and FAR is the percentage that unauthorized persons are accepted by the system [1]. The point where FAR and FRR have the same value is called Equal Error Rate (ERR).

The proposed system is dedicated for verification and therefore requires the user to claim identity through an artificial ID (e.g., magnetic card or PIN) before the system can start process of enrollment or authentication. Due to assistance of artificial IDs, verification systems require considerable less computational resources but the FRR may increase slightly. This is because the combined FRR for a system that uses both artificial IDs and biometric is:

$$FRR = FRR\ of\ ID + FRR\ of\ biometric\,. \tag{1}$$

On the other hand, the combined FAR can be greatly reduced with artificial identities:

$$FAR = FAR\ of\ ID \times FAR\ of\ biometric\,. \tag{2}$$

Requiring an artificial ID can minimize casual attacks to the biometric verification system because random claims can often be rejected as unknown to the database.

4. Enrollment

4.1 Image Capture

Enrollment involves a process of adding users to the database. The image acquisition system which we have designed (inspired from [4], [5]) comprises of a scanner and a flat surface. A user places his right hand on the surface of the device. The palm is facing downwards and the pegs are used as control points for fixing the appropriate position of the hand. To obtain an image, scanner is used in the next step (Fig. 1). Before obtaining a new hand picture, the user was instructed to remove the whole hand from the surface. This multiple placements allow the system to capture images of the hand in slightly different positions. That's also the other advantage compared to behavioral-based methods, because enrollment can be done in short time. For example, in case of voice recognition system, the process of enrollment must be realized in a long time period to include all possible aspects influencing the voice.

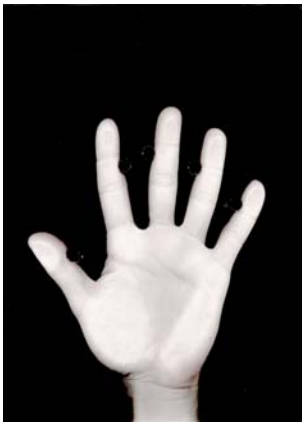

Fig. 1. Template captured by scanner.

The final database contains 26 people, where for every user 20 templates were captured. Because of possible incorrect placement of hand during enrolment, the best pictures have been chosen and 17 templates for each of the users left. The 15 of them are used for process of training and 2 of them for testing the system. Database consists of people of different sex and young ages.

4.2 Preprocessing

After the image is captured, it is preprocessed to obtain only the area information of the hand. The first step in preprocessing is its transforming to binary image. Since there is clear distinction in intensity between the hand and the background, a binary image is obtained through MATLAB function *im2bw*. The output binary image has values of 0 (black) for all pixels in the input image with luminance less than a level and 1 (white) for all other pixels. The level is a normalized intensity value obtained by Otsu's method, which chooses the threshold to minimize the intraclass variance of the black and white pixels.

Background lightning effects and the noise make fake pixels in the image. MATLAB function *imfilter* is used to remove these pixels and to justify edges of the hand in the next step. The function provides filtering of multidimensional images. The *imfilter* function computes the value of each output pixel using double-precision, floating-point arithmetic. Input image pixel values outside the bounds of the image are assumed to equal to the nearest array border value. Hand boundary is easily located afterwards.

4.3 Feature Extraction

Preprocessing simplifies a measurement algorithm and enables us to get features of the hand. An algorithm for feature extraction was created in programming environment MATLAB and it is based on counting pixel distances in specific areas of the hand. Since the system uses special surface with pegs to fix the appropriate position of the hand, it can obtain pixel distance of the given measurement. The algorithm looks for white pixels between two given points and computes a distance using geometrical principles. The result is a vector of 21 elements (Fig. 2):

- Widths: each of the fingers is measured in 3 different heights. Thump finger is measured in 2 heights.
- Heights: the height of all fingers and thumb is obtained.
- Palm: 2 measurements of palm size.

5. Recognition

The feature vector obtained by the verification should enter a comparison process to determinate if the person whose hand image was taken is the user who claims to be. This comparison is made against user model, which will be calculated depending on the comparison algorithm used. Experiments were made with different methods: Euclidian distance, Hamming distance, and Gaussian mixture model.

5.1 Euclidian Distance

Euclidian distance, considered the most common technique of all, performs its measurements with following equation:

$$d = \sqrt{\sum_{i=1}^{L} (x_i - t_i)^2} \tag{3}$$

where L is the dimension of the feature vector, x_i is the i-th component of the template feature vector, and t_i is the the i-th component of the model feature vector. Model in this case, is then represented as the mean of the resulting set of feature vectors.

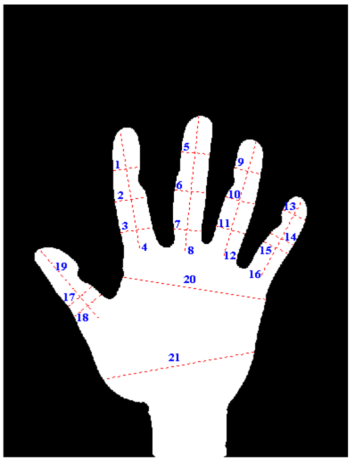

Fig. 2. Image after preprocessing and location of measurement points for feature extraction.

5.2 Hamming Distance

Hamming distance does not measure the difference between the components of the feature vectors, but the number of components that differ in value. As it is typical that all the components differ between samples of the same user, it is necessary to follow another approach for the template calculation different from one used for the Euclidian distance. Based on the assumption that the feature components follow normal distribution, not only the mean of the set of initial samples is obtained, but also a factor of standard deviation of the samples. In the comparison process, the number of components of the feature vector falling outside the area defined by the model parameters (represented by mean and standard deviation) is counted, obtaining the Hamming distance.

5.3 Gaussian Mixture Model

In order to obtain better results than in previous approaches, technique of Gaussian mixture models (GMM) has been implemented for recognition block. GMM is pattern recognition technique that uses an approach of the statistical methods [6]. The vector of each hand measurement can be described by normal distribution, also called Gaussian distribution. Each hand measurement may be then defined by two parameters (for our case, where measurement vector is one dimensional): mean (average) and standard deviation (variability). Suppose that the measurement vector is the discrete random variable x. For the general case, where vector is multidimensional, the probability density function of the normal distribution is a Gaussian function [2]:

$$p(x,\mu,\Sigma) = \frac{1}{\sqrt{(2\pi)^L |\Sigma|}} \exp^{\frac{(x-\mu)^T}{2\Sigma(x-\mu)}} \tag{4}$$

where μ is the mean, Σ is the covariance matrix and L is the dimension of feature vector. Covariance matrix is the natural generalization to higher dimensions of the concept of the variance of a random variable. If we suppose the random variable measurement is not characterized only with simple Gaussian distribution, we can then define it with multiple Gaussian components. GMM is a probability distribution that is a convex combination of other Gaussian distributions [2]):

$$p(x) = \sum_{j=1}^{J} \pi^{(j)} p\left(x, \mu^{(j)}, \Sigma^{(j)}\right) \tag{5}$$

where J is the number of Gaussian mixtures and $\pi^{(j)}$ is the weight of each of the mixture. After GMM is trained, the model of each user will be the final values of $\pi^{(j)}$, $\mu^{(j)}$, $\Sigma^{(j)}$ and J, which greatly increases the database size. Tab.1 shows the differences in the size of the model depending on the computational methods used.

Method used	Raw template	Euclidian distance	Hamming distance	GMM 2 mixtures
Model size	1,395 MB	352 B	520 B	1,209 kB

Tab. 1. Comparison of the model sizes for different techniques.

5.3.1 Expectation-Maximization Algorithm

To estimate the density parameters of a GMM statistic model, cluster estimation method called Expectation-maximization algorithm (EM) is adopted. The EM is the ideal candidate for solving parameter estimation problems for the GMM. Each of the EM iterations consists of two steps – Estimation (E) and Maximization (M). The M-step maximizes a likelihood function that is refined in each iteration by the E-step.

The GMM parameters can be divided into two groups: one containing $\pi^{(j)}s$ and another containing $\mu^{(j)}s$ and $\Sigma^{(j)}s$. The former indicates the importance of individual mixture densities via the prior probabilities $\pi^{(j)}s$, whereas the latter is commonly regarded as the kernel parameter defining the form of mixture density. Unlike other optimization technique in which unknown parameters can be arranged in any order, the EM approach effectively makes use of the structural relationship among the unknown parameters to simplify the optimization process. After initialization of parameters, the EM iteration is as follows:

1. The E-step determines the best guess of the membership function $h_n^{(j)}(x_t)$, which is the function for each element of x and each mixture [1]:

$$h_n^{(j)}(x_t) = \frac{p\left(x_t / \delta^{(j)} = 1, \phi_n^{(j)}\right)\pi_n^{(j)}}{\sum_{k=1}^{J} p\left(x_t / \delta^{(k)} = 1, \phi_n^{(k)}\right)\pi_n^{(k)}} \tag{6}$$

where $x_t/\delta_j=1$ defines that x_t is generated by the *j-th* mixture, ϕ_j is density function associated with the *j-th* mixture.

2. The M-step maximizes function to find new parameters $\pi^{(k)*}$, $\mu^{(k)*}$, $\Sigma^{(k)*}$ using (5), (6), (7). After that algorithm increment n by 1 and repeat E-step until convergence [1].

$$\mu^{(k)*} = \frac{\sum_{t=1}^{T} h_n^{(k)}(x_t).x_t}{\sum_{t=1}^{T} h_n^{(k)}(x_t)}, \tag{7}$$

$$\Sigma^{(k)*} = \frac{\sum_{t=1}^{T} h_n^{(k)}(x_t)\left(x_t - \mu^{(k)*}\right)\left(x_t - \mu^{(k)*}\right)^T}{\sum_{t=1}^{T} h_n^{(k)}(x_t)}, \tag{8}$$

$$\pi^{(k)*} = \frac{1}{T}\sum_{t=1}^{T} h_n^{k}(x_t). \tag{9}$$

After convergency of the main model parameters, the multiple Gaussian distributions can be described by one single function. In the case in Fig.3, the GMM has seven mixtures and two dimensional feature vector.

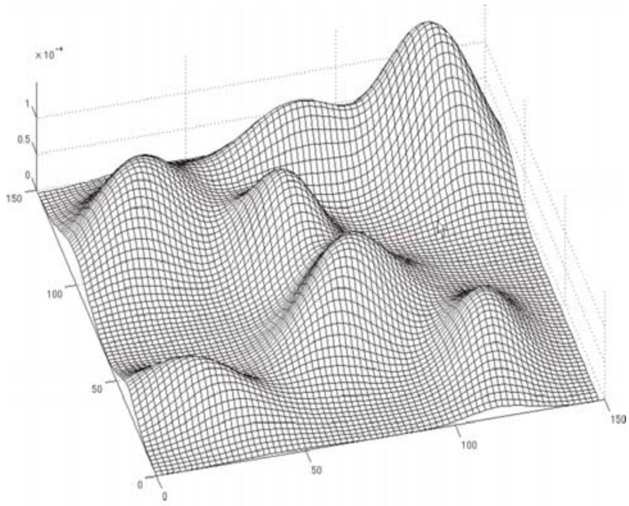

Fig. 3. GMM model - superposition of seven Gaussian distributions. Vertical axe represents probability density, and parameters on the horizontal axes are observations of 2-dimensional vector.

6. Experimental Results

System has been tested on the database described in section 4.1 totally with 408 hand templates. System behavior can be managed depending on environment for its using and security policy. This is done by a threshold, which influences both values, FAR and FRR. The threshold for GMM method is a value, which is compared to the probability obtained from GMM for a given user. If the probability offered by GMM is higher than the threshold, verification of the given user is positive, and vice versa. Likewise, the threshold for Euclidian distance or Hamming distance is a value, which is compared to the distance obtained from the recognition process. If the Euclidian or Hamming distance is lower than the threshold, verification is positive. The best values of FRR, FAR and ERR achieved for different computational methods are shown in Tab.2. The system was tested with different thresholds depending on used methods and the results in Tab.2 are the best achieved values.

	FRR (%)	FAR (%)	ERR (%)
GMM	14,583	0,1812	4,62
ED	10,417	0,272	6,45
HD	12,5	4,0761	9,73

Tab. 2. Results for different methods: GMM – Gaussian Mixture Model, ED – Euclidian distance, HM – Hamming distance.

As mentioned above, tradeoff between FAR and FRR is adjusted by a threshold, which needs to be adjusted carefully so that the two rates can both satisfy the prescribed security standards. If a security system makes users feel uncomfortable, either psychologically or physically, then the system is intrusive. For example, in computer network security or access control for areas requiring middle or low security levels, an intrusive system will annoy users and therefore will discourage them from using it. In high security areas, an intrusive system sometimes can turn out to be a benefit, since it may appear to be a highly secure recognition method. This elevated sense of security may in itself discourage intruders. Tab.3 and Fig. 4 show FRR and FAR values dependent on the adjustable adopted threshold for method GMM. Due to a small value of the threshold, it is given by a negative logarithmic value.

GMM (2 mixtures)		
Threshold (-log)	FRR (%)	FAR (%)
21,1864	16,667	0,0906
30,1863	14,583	0,1812
87,0676	8,333	3,0797
116,1882	0,1	6,4312

Tab. 3 Values FAR and FRR dependent on adjusted security threshold.

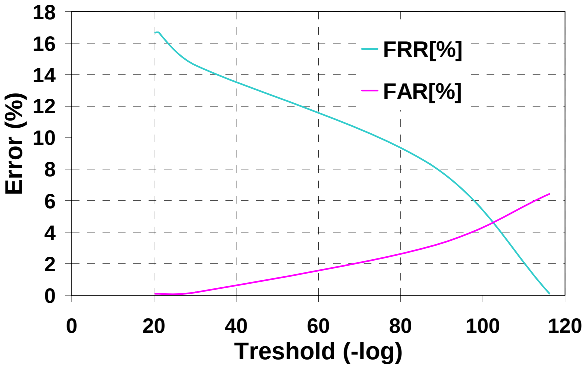

Fig. 4. FAR and FRR against threshold.

In order to reach an effective comparison of different systems, the description independent of threshold scaling is required. Receiver Operating Characteristic (ROC) in Fig.5 plots FRR values directly against FAR values and eliminates threshold parameters.

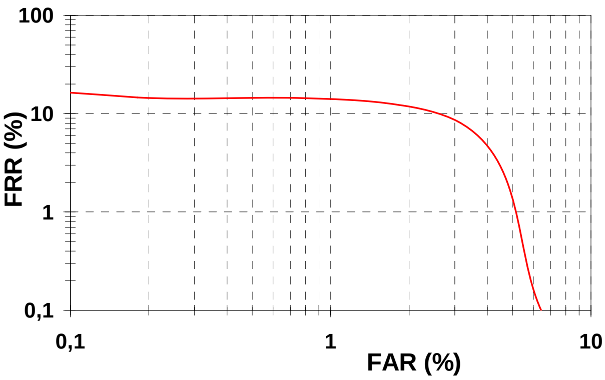

Fig. 5. Receiver Operating Characteristic (ROC).

7. Conclusion

Experiments presented show the possibilities of using hand geometry as the biometric characteristic for automatic verification systems. Hand geometry features used for the proposed system were shown as enough unique to use them to verify the person's identity. From the comparison methods, Gaussian mixture modeling has been revealed as the one with the best performance and became preferred to Euclidean and Hamming distance. The best results achieved GMMs with 2 mixtures: FAR=0,1812%, FRR=14,583% and EER=4,62%. All users showed great acceptance and easy of usage of the system during process of enrollment and creating the database. This system as designed currently is considered a good alternative for security applications for areas requiring middle or low security levels (e.g., apartments, hospitals, stores, attendance). Further work should be applied to create multimodal biometric system with a fusion of hand geometry and voice print techniques to get security system with high accuracy.

Acknowledgements

The research described in the paper was supported by the Ministry of Education and the Academy of Science of the Slovak republic VEGA under Grant No. 1/4054/07.

References

[1] KUNG, S. Y., MAK, M. W., LIN, S. H. *Biometric Authentication.* Published as Prentice Hall Professional Technical Reference. New Jersey: First Printing, September 2004.

[2] VARCHOL, P., LEVICKY, D. Implementation of Gaussian mixture models for biometric security system. In *Proceedings Komunikacne a informacne technologie,* Tatranske Zruby(Slovak Republic), 2007.

[3] VARCHOL, P., LEVICKY, D. Access security based on biometric. In *Proceedings Research in Telecommunication Technology.* Nove Mesto na Morave (Slovak Republic), 2006.

[4] SANCHEZ-REILLO, R. Biometric identification through hand geometry measurements. *IEEE Transactions on Pattern Analysis and Machine Intelligence.* ISSN: 0162-8828. Washington, 2000.

[5] JAIN, A., ROSS, A. A prototype hand geometry-based verification system. In *Proceedings of 2nd Int. Conference on Audio- and Video-based Biometric Person Authentication.* Washington (USA), 1999.

[6] YOUNG, S. *The HTK Book (for HTK Version 3.2).* First published December 1995, Revised for HTK Version 3.2 December 2002.

About Authors...

Dušan LEVICKÝ – for biography see p. 81 of this issue.

Peter VARCHOL was born in Stará Ľubovňa, Slovakia, in 1980. He graduated from the Technical University in Košice, Faculty of Electrical Engineering and Informatics. Since 2004 he has been PhD. student at the Department of Electronics and Multimedia Communications, focusing on biometric security, network technologies and digital image processing.

RADIOENGINEERING REVIEWERS

December 2007, Volume 16, Number 4

- BAUDOIN, G., ESIEE Paris, France
- BARDOŇOVÁ, J., Brno University of Technology
- BÁRTÍK, H., Czech Technical University in Prague
- BILÍK, V., Slovak University of Technology, Bratislava, Slovakia
- ĎAĎO, S., Czech Technical University in Prague
- DJIGAN, V., ELVEES R&D Center of Microelectronics, Moscow, Russia
- DOLEŽEL, I., Czech Technical University in Prague
- DRUTAROVSKÝ, M., Technical University of Košice, Slovakia
- DŘÍNOVSKÝ, J., Brno University of Technology
- FRÝZA, T., Brno University of Technology
- HALÁMEK, J., Academy of Sciences of the Czech Republic, Brno
- HEMZAL, D., Masaryk University, Brno
- HOZMAN, J., Czech Technical University, Kladno
- JIŘÍK, R., Brno University of Technology
- KLÍMA, M., Czech Technical University in Prague
- KOLÁŘ, R., Brno University of Technology
- KOTULIAKOVÁ, J., Slovak University of Technology, Bratislava, Slovakia
- KOZUMPLÍK, J., Brno University of Technology
- KRATOCHVÍL, T., Brno University of Technology
- KRŠEK, P., Brno University of Technology
- KULLA, P., Slovak University of Technology, Bratislava, Slovakia
- LÁČÍK, J., Brno University of Technology
- LEVICKÝ, D., Technical University of Košice, Slovakia
- LUKEŠ, Z., Brno University of Technology
- MACHÁČ, J., Czech Technical University in Prague
- MARŠÁLEK, R., Brno University of Technology
- MIHALÍK, J., Technical University of Košice, Slovakia
- NOVOTNÝ, V., Brno University of Technology
- PÁTA, P., Czech Technical University in Prague
- PECHAČ, P., Czech Technical University in Prague
- PETRŽELA, J., Brno University of Technology
- POLEC, J., Slovak University of Technology, Bratislava, Slovakia
- POLÍVKA, M., Czech Technical University in Prague
- POMĚNKA, P., TheNet, Brno
- PROKEŠ, A., Brno University of Technology
- PROVAZNÍK, I., Brno University of Technology
- RAJMIC, P., Brno University of Technology
- SCHEJBAL, V., University of Pardubice
- ŠEBESTA, V., Brno University of Technology
- ŠŤASTNÝ, J., Czech Technical University in Prague
- URBANEC, T., Brno University of Technology
- VARGIC, R., Slovak University of Technology, Bratislava, Slovakia
- WIESER, V., University of Žilina, Slovakia
- ZAVACKÝ, J., Technical University of Košice, Slovakia
- ZEMČÍK, P., Brno University of Technology
- ŽALUD, V., Czech Technical University in Prague