E

Ear Biometrics

Michal Choras
Image Processing Group, Institute of Telecommunications, University of Technology and Life Sciences, Bydgoszcz, Poland

Definition

The term ear biometrics refers to automatic human identification on the basis of the ear physiological (anatomical) features. The identification is performed on the basis of the features which are usually calculated from captured 2D or 3D ear images (using pattern recognition and image processing techniques). The ear features that can be used in the process of identification are, for example, geometrical ear structure, characteristic ear points, global ear image features, local ear image features, and 3D models. The advantages of human ear as biometric as well as the overview of various approaches to ear biometrics are presented in the ear biometrics overview entry.

Introduction

As pointed out by Hurley et al., ear biometrics is no longer in its infancy and has shown encouraging progress [1]. It is due to the fact that the ear is the very interesting human anatomical part for **passive** physiological biometric systems. It means that the subject does not have to take active part in the whole process or, in fact, would not even know that the process of identification takes place.

There are many advantages of using the ear as a source of data for human identification. Firstly, the ear has a very rich structure of characteristic ear parts. The location of these characteristic elements, their direction, angles, size, and relation within the ear are distinctive and unique for humans and, therefore, may be used as a modality for human identification [2, 3]. The ear is one of the most stable human anatomical features. It does not change considerably during human life, while face changes more significantly with age than any other part of human body [2, 3]. Face can also change due to cosmetics, facial hair, and hairstyling. Secondly, human faces change due to emotions and express different states of mind like sadness, happiness, fear, or surprise. In contrast, ear features are fixed and unchangeable by emotions. The ear is not symmetrical – the left and right ears are not the same. Due to forensics and medical studies, from the age of four, ears grow proportionally, which is the problem of scaling in computer vision systems [2].

Furthermore, the ear is a human sensor; therefore, it is usually visible to enable good hearing. In the process of acquisition, in contrast to face identification systems, ear images cannot be disturbed by glasses, beard, or makeup. However, occlusion by hair or earrings is possible. It is worth to mention that ear images are more

S.Z. Li, A.K. Jain (eds.), *Encyclopedia of Biometrics*, DOI 10.1007/978-1-4899-7488-4,

secure than face images, mainly because it is very difficult to associate ear image with a given person (in fact, most of users are not able to recognize their own ear image). Therefore, any attacks on privacy (such as identity theft) are not very probable by means of using ear images.

On the other hand, ear biometrics is not a natural way of identifying humans. In real life we do not look at people's ears to recognize them. Our identification decision is rather based on faces, voice, or gait. The reason is that people lack in vocabulary to describe ears – would anyone describe spouse or sibling ears in detail? The main task of ear biometrics is to define such vocabulary – in context of the computer vision systems, such vocabulary is called "features." In ear biometrics computer vision systems, the main task is to extract such features that will describe human ears in a distinctive way.

In the following sections the selection of various approaches to extract features from 2D and 3D ear images will be shortly presented.

2D Ear Biometrics

Geometrical Approach to Feature Extraction

The first to explore the possibility of using ear as a biometric in a computer vision system were **Burge and Burger** [4]. They presented the geometrical method based on building neighborhood graphs and Voronoi diagrams of the detected edges. Additionally, **Burge and Burger** pointed out that thermal imaging may solve the problem of ear occlusion (mainly by hair). They proposed to use segmentation algorithm based on color and texture of **ear thermogram**.

Choraś developed several methods of geometrical feature extraction from ear images [5]. The proposed "geometrical parameter methods" had been motivated by actual procedures used in the police and forensic evidence search applications. In reality, procedures of handling ear evidence (earprints and/or ear photographs) are based on geometrical features such as size, width, height, and earlobe topology [2]. Choraś developed and tested several methods in order to extract distinctive geometrical features from human ear 2D images. Moreover, in Choraś work the contour detection algorithm and the method of ear contour image processing in order to select the most meaningful contours have been developed. Choraś' methods were tested in laboratory conditions, while the ear image database was created in the controlled environment.

Yuan and Tian presented ear contour detection algorithm based on local approach [6]. Edge tracking is applied to three regions in which contours were extracted in order to obtain clear, connected, and non-disturbed contour, which may be further used in the recognition step. **Sibai et al.** used artificial neural networks (ANN) fed with seven manually selected and calculated geometrical features [7].

SIFT

Arbab-Zavar et al. proposed to use Scale Invariant Feature Transform (*SIFT*) to extract the ear salient points and to create human ear model later used in recognition [8]. Their ear model is constructed using a stochastic method. In their experiments they proved that using ear model outperforms *PCA* method in case of occluded ears. **Zhou et al.** used the fusion of color SIFT features calculated in R, G, and B color channels [9]. **Kisku et al.** proposed SIFT features calculated on ear images modeled by Gaussian mixture model and Kullback-Leibler divergence [10]. Fusion of SIFT features calculated for various ear poses (at angles −40, −20, 0, 20, 40) was proposed by **Badrinath and Gupta** in [11].

Global Features

Principal component analysis, force field transformations, and wavelets have been applied to ear biometrics human identification. Recently, the idea of recognition based on ear models gained some popularity and attention.

Victor et al. used principal component analysis (*PCA*) in the experiment comparing ear and face properties in order to successfully identify humans in various conditions [12]. In case of faces, the authors perform recognition on the basis of *eigenfaces*. In case of ear biometrics,

the authors used a set of *eigenears*. Their work proved that ear images are a very suitable source of data for identification and their results for ear images were not significantly different from those achieved for face images. The proposed methodology, however, was not fully automated, since the reference (so-called landmark points) had to be manually inserted into images. In case of ear images, these landmark points are manually marked in the triangular fossa and in the point known as antitragus. **Hurley et al.** introduced a method based on energy features of the 2D image [13]. They proposed to perform force field transformation (step 1) in order to find energy lines, channels, and wells (step 2). Recently, in **Cummings et al.** the usefulness of image ray transform (IRT) for ear detection was shown [14]. **Moreno et al.** presented another approach to ear image feature extraction [15]. Their work was based on macrofeatures extracted by compression networks. Several neural network methods and classifiers based on 2D intensity images were presented: compression networks, Borda combination, Bayesian, and weighted Bayesian combination. The best results of 93 % were achieved by the compression network ear identification method. **Sana et al.** developed a new approach to ear biometrics based on Haar wavelets [16]. After ear detection step, Haar wavelet transformation is applied and wavelet coefficients are computed. They performed their experiments on two ear datasets (from Indian Institute of Technology Kanpur and from Saugor University) and report accuracy of about 96 % on both databases. **Lu et al.** used active shape models (*ASM*) to model the shape and local appearances of the ear in a statistical form [17]. Then *eigenears* have been also used in a final classification step. They used both left and right ear images and showed that their fusion outperforms results achieved for single ears separately. They achieved 95.1 % recognition rate for double ears. **Yuan and Mu** also explored the advantages of improved active shape models (*ASM*) to the task of ear recognition [18]. They applied their algorithm to the rotation-invariance experiment. The interesting contribution of their work is the comparison of right and left rotations of the same ears. They found out that right head rotation of 20° is acceptable for recognition. For left head rotation, the acceptable angle is 10°. Recently, **Yuan and Mu** proposed another approach based on fusion of local features calculated by neighborhood preserving embedding (NPE) in sub-windows, later treated as sub-classifiers [19]. Lately, the sparse representation (SR) has drawn some attention and was used for feature extraction by **Huang et al.** [20] and **Kumar and Chan** [21].

Gabor-Based Features

Many recent developments in ear biometrics use properties of Gabor and log-Gabor-based features. **Xu** used Gabor wavelets to calculate global features of ear images and then classified the feature vectors using support vector machines (SVM) [22]. **Arab-Zavar and Nixon** used log-Gabor filters (also SIFT) for model-based ear recognition [23]. SIFT method was useful for inner parts of ear models, while log-Gabor particularly for outer curves. **Liu** proposed to use log-Gabor features applied to force field convergence map of ear image [24]. **Yazdanpanah and Faez** proposed Gabor-based region convergence matrix (RCM) for ear feature calculation [26]. Gabor filters are also used by **Nanni and Lumini** in [27] where authors also use properties of color spaces (RGB and YIQ). **Chan and Kumar** used 2D quadrature filtering (quaternionic and monogenic) methods and proposed Quaternionic Code-based ear image description which was described and tested in [28].

3D Ear Recognition

Recently, the possibility of human identification on the basis of 3D images has been extensively researched. Various approaches towards multimodal 2D + 3D ear biometrics as well as 3D ear biometrics, mainly based on *ICP* (iterative closest point), have been recently developed and published [29–32].

Chen and Bhanu proposed 3D ear recognition based on local shape descriptor as well as two-step *ICP* algorithm. Additionally, they developed the algorithm to detect ear regions

Ear Biometrics, Fig. 1 Examples of easy ear images [25]

Ear Biometrics, Fig. 2 Examples of difficult ear images [25]

from 3D range images. They collected their own ear image database (UCR database) consisting of 902 images from 302 subjects. Their results of ear detection, matching, and identification are close to 100 % recognition rate [29]. **Yan and Bowyer** developed three approaches to 3D ear recognition problem: edge based, *ICP*, and $3D - PCA$. Moreover, they tested various approaches (e.g., 2D + 3D) in multimodal biometric scenario [30]. They designed fully automated ear recognition system and achieved satisfactory results of 97.6 % Rank-1 recognition. In their research they did not exclude partially occluded ears or ears with earrings. They performed experiments on the largest ear database collected so far. UND ear database is now becoming a standard ear database for ear recognition experiments. **Cadavid and Abdel-Mottaleb** built 3D ear models from captured video frames. Then they used "structure from motion" (*SFM*) and "shape from shading" (*SFS*) techniques to extract 3D ear characteristics [31]. They were first to explore the 3D ear biometrics based on video sequences, not on images acquired by 3D range scanners. **Zhou et al.** proposed 3D system using local and holistic features, such as histogram of indexed shapes (HIS) and surface path histogram of indexed shapes (SPHIS) [32].

Conclusion

Human ear is a perfect source of data for passive person identification in many applications. In a growing need for security in various public places, ear biometrics seems to be a good solution, since ears are visible and their images can be easily taken, even without the examined person's knowledge.

It is noticeable that even though all of the proposed techniques are developed to solve the same image processing task, many totally

different methodologies and algorithms have been developed.

Such situation proves that ear biometrics has lately gained much interest and popularity in computer science community. It also may be the indication that ear biometrics will become one of the standard means of human identification in unimodal or hybrid biometrics systems.

Currently, ear biometrics developments shift from introductory works to solving challenging problems in non-controlled realistic ear images such as occlusion and pose variations.

Ear Biometrics, Table 1 Feature extraction approaches for ear biometrics

Research group	Proposed methodology
Burge and Burger	2D – Voronoi diagrams
Choraś	2D – geometrical methods
Sibai et al.	2D – 7 (manual) geometrical features, ANN
Arbab-Zavar	2D – SIFT, model
Zhou et al.	2D – SIFT in color spaces
Kisku et al.	2D – SIFT, GMM, K-L divergence
Badrinath and Gupta	2D – SIFT
Victor et al.	2D – PCA
Hurley et al.	2D – force field transformation
Cummings et al.	2D – image ray transform
Lu et al.	2D – ASM
Moreno et al.	2D – compression networks
Sana et al.	2D – Haar wavelets
Yuan and Mu	2D – ASM
Yuan and Mu	2D – local fusion, NPE
Huang et al.	2D – sparse representation
Kumar and Chan	2D – sparse representation
Xu	2D – Gabor wavelets, SVM
Arab-Zavar and Nixon	2D – log-Gabor
Liu	2D – log-Gabor, force field convergence map
Yazdanpanah and Faez	2D – Gabor-based RCM
Nanni and Lumini	2D – Gabor filters, color spaces
Chan and Kumar	2D – quadrature filtering
Chen and Bhanu	3D – ICP and shape descriptors
Yan and Bowyer	3D – ICP, edge based, and PCA
Cadavid and Abdel-Mottaleb	3D – SFM, SFS
Zhou et al.	3D – HIS, SPHIS

Ear biometrics can also be used to enhance effectiveness of other well-known biometrics, by its implementation in multimodal systems. Since most of the methods have some drawbacks, the idea of building multimodal (hybrid) biometrics systems is gaining lot of attention [33]. Due to its advantages, ear biometrics seems to be a good choice to support well-known methods like voice, gait, hand, palm, and most often face identification.

The summary of the research groups with the proposed approaches and methods is given in Table 1.

Summary

In this entry the holistic overview of ear recognition methods for biometrics applications is presented. 2D and 3D image processing algorithms applied to ear feature extraction are surveyed. In this work strong motivation for using the ear as a biometrics is given, and afterwards, various approaches to 2D ear biometrics and 3D ear biometrics are presented.

Related Entries

▸ Ear Biometrics, 3D
▸ Ear Recognition, Physical Analogies

References

1. D.J. Hurley, B. Arab-Zavar, M.S. Nixon, The ear as a biometric, in *Proceedings of Eusipco'07*, Poznan, 2007, pp. 25–29
2. J. Kasprzak, *Forensic Otoscopy (in Polish)* (University of Warmia and Mazury Press, Olsztyn, 2003)
3. A. Iannarelli, *Ear Identification*. Forensic Identification Series (Paramont Publishing Company, Fremont, 1989)
4. M. Burge, W. Burger, Ear biometrics, in *Biometrics: Personal Identification in Networked Society*, ed. by A.K. Jain, R. Bolle, S. Pankanti (Kluwer, Dordecht, 1998), pp. 273–286
5. M. Choraś, Perspective methods human identification: ear biometrics. Opto-Electron. Rev. **16**(1), 49–60 (2008)

6. W. Yuan, Y. Tian, Ear contour detection based on edge tracking, in *Proceedings of Intelligent Control and Automation*, Dalian (IEEE, 2006), pp. 10450–10453
7. F.N. Sibai, A. Nuaimi, A. Maamari, R. Kuwair, Ear recognition with feed-forward artificial neural networks. Neural Computing and Applications, **23**(5), pp. 1265–1273 (2013). Springer, 2013
8. B. Arab-Zavar, M.S. Nixon, D.J. Hurley, On model-based analysis of ear biometrics, in *Proceedings of IEEE Conference on Biometrics: Theory, Applications and Systems – BTAS'07*, Washington, DC, 2007
9. J. Zhou, S. Cadavid, M. Abdel-Mottaleb, Exploiting color SIFT features for 2D ear recognition, in *Proceedings of International Conference on Image Processing*, Brussels (IEEE, 2011), pp. 553–556
10. D. Kisku, H. Mehrotra, P. Gupta, J.K. Sing, SIFT-based ear recognition by fusion of detected keypoints from color similarity slice regions, in *Proceedings of IEEE ACTEA*, Lebanon, 2009, pp. 380–385
11. G.S. Badrinath, P. Gupta, Feature level fused ear biometric system, in *Proceedings of Advances in Pattern Recognition*, Kolkata (IEEE, 2009), pp. 197–200
12. B. Victor, K.W. Bowyer, S. Sarkar, An evaluation of face and ear biometrics, in *Proceedings of International Conference on Pattern Recognition*, Quebec City, 2002, pp. 429–432
13. D.J. Hurley, M.S. Nixon, J.N. Carter, Force field energy functionals for ear biometrics. Comput. Vis. Image Underst. **98**(3), 491–512 (2005)
14. A.H. Cummings, M.S. Nixon, J.N. Carter, The image ray transform for structural feature detection. Pattern Recognit. Lett. **32**, 2053–2060 (2011)
15. B. Moreno, A. Sanchez, J.F. Velez, On the use of outer ear images for personal identification in security applications, in *Proceedings of IEEE Conference on Security Technologies*, Madrid, 1999, pp. 469–476
16. A. Sana, P. Gupta, R. Purkai, Ear biometrics: a new approach, in *Advances in Pattern Recognition*, Kolkata, ed. by P. Pal (World Scientific Publishing, 2007), pp. 46–50
17. L. Lu, X. Zhang, Y. Zhao, Y. Jia, Ear recognition based on statistical shape model, in *Proceedings of International Conference on Innovative Computing, Information and Control*, Beijing, vol. 3 (IEEE, 2006), pp. 353–356
18. L. Yuan, Z. Mu, Ear recognition based on 2D images, in *Proceedings of IEEE Conference on Biometrics: Theory, Applications and Systems – BTAS'07*, Washington, DC, 2007
19. L. Yuan, Z. Mu, Ear recognition based on local information fusion. Pattern Recognit. Lett. **33**, 182–190 (2012)
20. Z. Huang, Y. Liu, Ch. Li, M. Yang, L. Chen, A robust face and ear based multimodal biometric system using sparse representation. Pattern Recognit. **46**, 2156–2168 (2013)
21. A. Kumar, T.-S.T. Chan, Robust ear identification using sparse representation of local texture descriptors. Pattern Recognit. **46**, 73–85 (2013)
22. H. Xu, The research of ear recognition based on Gabor wavelets and support vector machine classification. Information Technology Journal, **11**, 1626–1631 (2012)
23. B. Arab-Zavar, M. Nixon, On guided model-based analysis of ear biometrics. Comput. Vis. Image Underst. **115**, 487–502 (2011)
24. H. Liu, Force field convergence map and log-Gabor filter based multi-view ear feature extraction. Neurocomputing **76**, 2–8 (2012)
25. M. Choraś, Ear biometrics based on geometrical method of feature extraction, in *Articulated Motion and Deformable Objects*, ed. by F. J. Perales, B. A. Draper. LNCS 3179 (Springer, Berlin, 2004), pp. 51–61
26. A.P. Yazdanpanah, K. Faez, Gabor-based RCM features for ear recognition, in *State of the Art in Biometrics*, ed. by J. Yang (Intech, 2011), pp. 221–234
27. L. Nanni, A. Lumini, Fusion of color spaces for ear authentication. Pattern Recognit. **42**, 1906–1913 (2009)
28. T.-S. Chan, A. Kumar, Reliable ear identification using 2-D quadrature filters. Pattern Recognit. Lett. **33**, 1870–1881 (2012)
29. H. Chen, B. Bhanu, Human ear recognition in 3D. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 718–737 (2007)
30. P. Yan, K.W. Bowyer, Multi-biometrics 2D and 3D ear recognition, in *Proceedings of Audio- and Video-Based Biometric Person Authentication*, Hilton Rye Town, 2005, pp. 503–512
31. S. Cadavid, M. Abdel-Mottaleb, Human identification based on 3D ear models, in *Proceedings of IEEE Conference on Biometrics: Theory, Applications and Systems – BTAS'07*, Washington, DC, 2007
32. J. Zhou, S. Cadavid, M. Abdel-Mottaleb, An efficient 3-D ear recognition system employing local and holistic features. IEEE Trans. Inf. Forensics Secur. **7**(3), 978–991 (2012)
33. A. Ross, K. Nandakumar, A.K. Jain, *Handbook of Multibiometrics*. International Series on Biometrics (Springer, Berlin, 2006)

Ear Biometrics, 3D

Bir Bhanu and Hui Chen
Center for Research in Intelligent Systems, University of California, Riverside, CA, USA

Synonyms

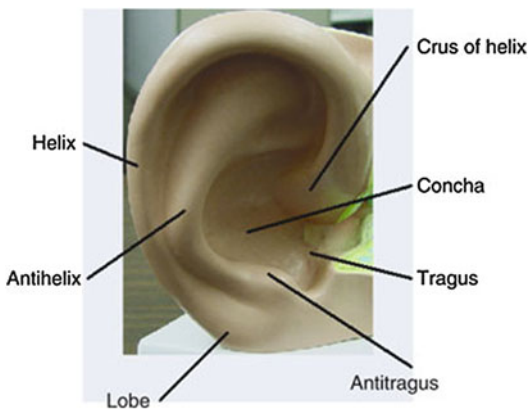
Ear recognition, 3D

Definition

The human ear is a new class of relatively stable biometrics. After decades of research of anthropometric measurements of ear photographs of thousands of people, it has been found that no two ears are alike, even in the cases of identical and fraternal twins, triplets, and quadruplets [1]. It is also found that the structure of the ear does not change radically over time. Ear biometric has played a significant role in forensic science and its use by law enforcement agencies for many years [1], but most of this work has been on analyzing the earprints manually. Recent work on ear biometrics focuses on developing automated techniques for ear recognition [2]. Ear biometrics can be based on a 2D gray scale or color image, 3D range image, or a combination of 2D and 3D images. Typically, an ear biometric system consists of ear detection and ear recognition modules.

Introduction

Rich in features, the human ear is a stable structure that does not change much in shape with the age and with facial expressions (see Fig. 1). Ear can be easily captured from a distance without a fully cooperative subject, although it can sometimes be hidden by hair, muffler, scarf, and earrings. Researchers have developed several biometric techniques using the 2D intensity images of human ears [3–8].



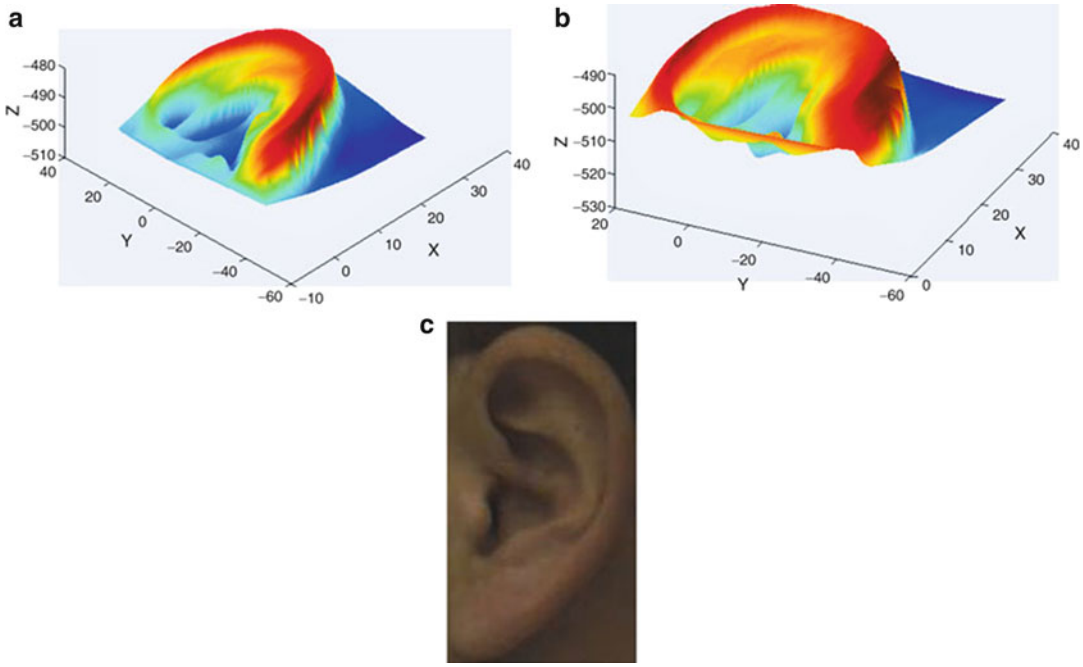
Ear Biometrics, 3D, Fig. 1 The external ear and its anatomical parts

Burge and Burger [3, 4] developed a computer vision system to recognize ears in the intensity images. Their algorithm consisted of four components: edge extraction, curve extraction, construction of a graph model from the Voronoi diagram of the edge segments, and graph matching. Hurley et al. [5] applied a force field transform to the entire ear image and extracted wells and channels. The wells and channels form the basis of an ear's signature. To evaluate differences among ears, they used a measure of the average normalized distance of the well positions, together with the accumulated direction to the position of each well point from a chosen reference point. Later, Hurley et al. [6] measured convergence to achieve greater potency in recognition. Chang et al. [8] used principal component analysis for ear and face images and performed experiments with face, ear, and face plus ear. Their results showed that multimodal recognition using both face and ear achieved a much better performance than the individual biometrics.

The performance of these 2D techniques is greatly affected by the pose variation and imaging conditions. However, ear can be imaged in 3D using a range sensor which provides a registered color and range image. Figure 2 shows an example of a range image and the registered color image acquired by a Minolta Vivid 300 camera. A range image is relatively insensitive to illuminations and contains surface shape information related to the anatomical structure, which makes it possible to develop a robust 3D ear biometrics. Examples of ear recognition using 3D data are [9–13]. The performance of 3D approaches for ear recognition is significantly higher than the 2D approaches. In the following, the chapter focuses on 3D approaches for ear detection and recognition.

Datasets

There are currently two datasets for 3D ear performance evaluation: the University of California at Riverside dataset (the UCR dataset) and the



Ear Biometrics, 3D, Fig. 2 Range image and color image captured by a Minolta Vivid 300 camera. In images (**a**) and (**b**), the range image of one ear is displayed as the shaded mesh from two viewpoints (the units of x, y, and z are in millimeters). Image (**c**) shows the color image of the ear

University of Notre Dame public dataset (the UND dataset). In the UCR dataset there is no time lapse between the gallery and probe for the same subject, while there is a time lapse of a few weeks (on the average) in the UND dataset.

UCR Dataset: The data [10] are captured by a Minolta Vivid 300 camera. This camera uses the light-stripe method to emit a horizontal stripe light to the object, and the reflected light is then converted by triangulation into distance information. The camera outputs a range image and its registered color image in less than 1 s. The range image contains 200 × 200 grid points, and each grid point has a 3D coordinate (x, y, z) and a set of color (r, g, b) values. During the acquisition, 155 subjects sit on a chair about 0.55–0.75 m from the camera in an indoor office environment. The first shot is taken when a subject's left-side face is approximately parallel to the image plane; two shots are taken when the subject is asked to rotate his or her head to the left and to the right side within ±35° with respect to his or her torso. During this process, there can be some face tilt as well, which is not measured. A total of six images per subject are recorded. A total of 902 shots are used for the experiments since some shots are not properly recorded. Every person has at least four shots. The average number of points on the side face scans is 23,205. There are three different poses in the collected data: frontal, left, and right. Among the total 155 subjects, there are 17 females. Among the 155 subjects, 6 subjects have earrings and 12 subjects have their ears partially occluded by hair (with less than 10 % occlusion).

UND Dataset: The data [13] are acquired with a Minolta Vivid 910 camera. The camera outputs a 480 × 640 range image and its registered color image of the same size. During acquisition, the subject sits approximately 1.5 m away from the sensor with the left side of the face toward the camera. In Collection F, there are 302 subjects with 302 time-lapse gallery-pro. Collection G contains 415 subjects, of which 302 subjects are

from Collection F. The most important part of Collection G is that it has 24 subjects with images taken at four different viewpoints.

Ear Detection

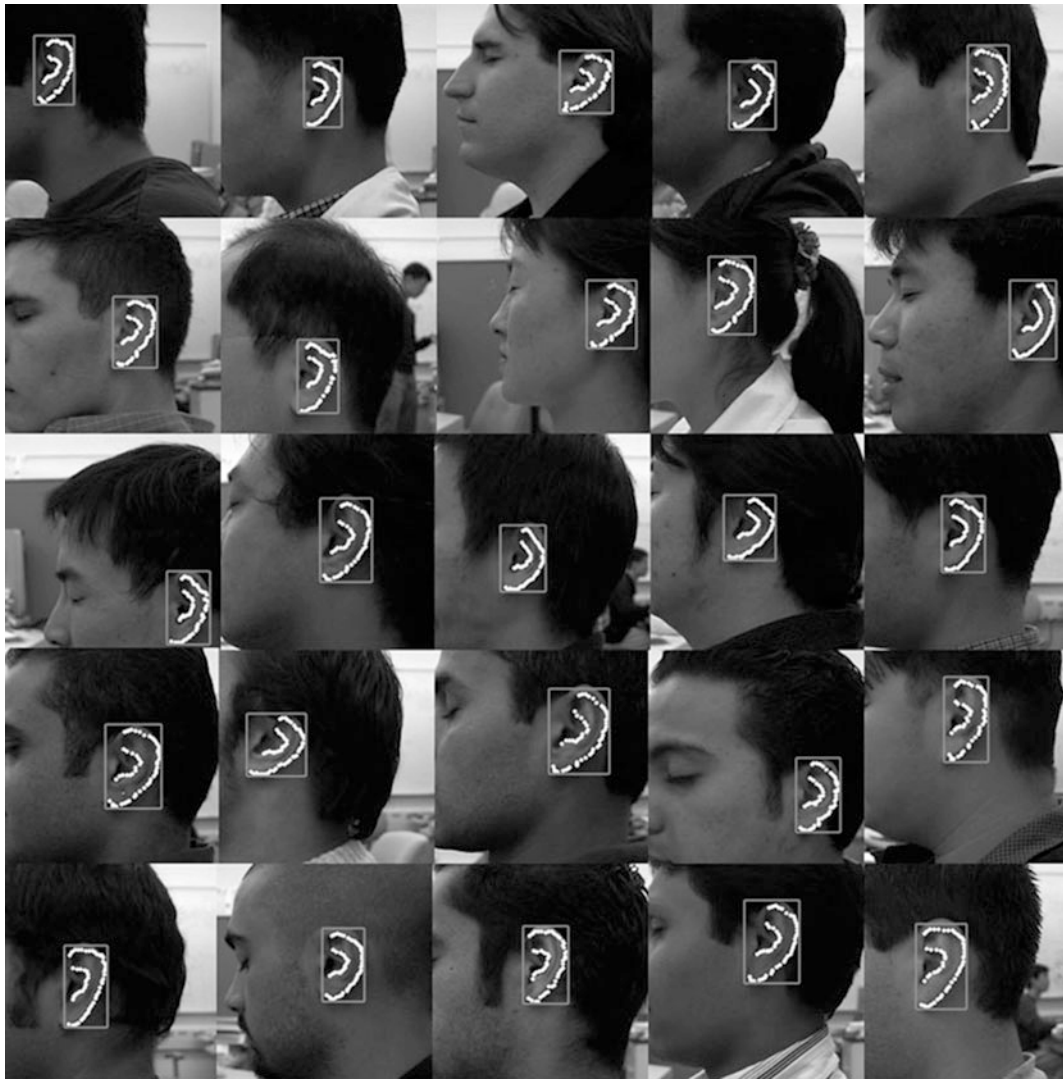
Human ear detection is the first task of a human ear recognition system, and its performance significantly affects the overall quality of the system. Automated techniques for locating human ears in side face range images are (i) template matching-based detection, (ii) ear shape model-based detection, and (iii) fusion of color and range images and global-to-local registration-based detection. The first two approaches use range images only, and the third approach fuses the color and range images.

The template matching-based approach has two stages: offline model template building and online ear detection. The ear can be thought of as a rigid object with much concave and convex areas. The averaged histogram of shape index (a quantitative measure of the shape of a surface) represents the ear model template. During the online detection, first the step edges are computed and thresholded since there is a sharp step edge around the ear boundary, and then image dilation and connected-component analysis is performed to find the potential regions containing an ear. Next, for every potential region, the regions are grown and the dissimilarity between each region's histogram of shape indexes and the model template is computed. Finally, among all of the regions, we choose the one with the minimum dissimilarity as the detected region that contains ear.

For the ear shape model-based approach, the ear shape model is represented by a set of discrete 3D vertices corresponding to ear helix and antihelix parts. Since the two curves formed by the ear helix and antihelix parts are similar for different people, we do not take into account the small deformation of two curves between different persons, which greatly simplifies the ear shape model. Given side face range images, first the step edges are extracted; then the edge segments are dilated, thinned, and grouped into different clusters which are the potential regions containing an ear. For each cluster, the ear shape model is registered with the edges. The region with the minimum mean registration error is declared as the detected ear region; the ear helix and antihelix parts are identified in this process.

In the above two approaches, there are some edge segments caused by non-skin pixels, which result in false detection. Since a range sensor provides a registered 3D range image and a 2D color image (see Fig. 2), it is possible to achieve a better detection performance by fusion of the color and range images. This approach consists of two steps for locating the ear helix and the antihelix parts.

In the first step a skin color classifier is used to isolate the side face in an image by modeling the skin color and non-skin color distributions as a mixture of Gaussians. The edges from the 2D color image are combined with the step edges from the range image to locate regions of interest (ROIs) that may contain an ear. In the second step, to locate an ear accurately, the reference 3D ear shape model, which is represented by a set of discrete 3D vertices on the ear helix and the antihelix parts, is adapted to individual ear images by following a global-to-local registration procedure instead of training an active shape model built from a large set of ears to learn the shape variation. In this procedure, after the initial global registration, local deformation process is carried out where it is necessary to preserve the structure of the reference ear shape model since neighboring points cannot move independently under the deformation due to physical constraints. The bending energy of thin plate spline, a quantitative measure for nonrigid deformations, is incorporated into the optimization formulation as a regularization term to preserve the topology of the ear shape model under the shape deformation. The optimization procedure drives the initial global registration toward the ear helix and the antihelix parts, which results in the one-to-one correspondence of the ear helix and the antihelix between the reference ear shape model and the input image. Figure 3 shows various examples in which the detected ear helix and the antihelix parts are shown by the dots superimposed on

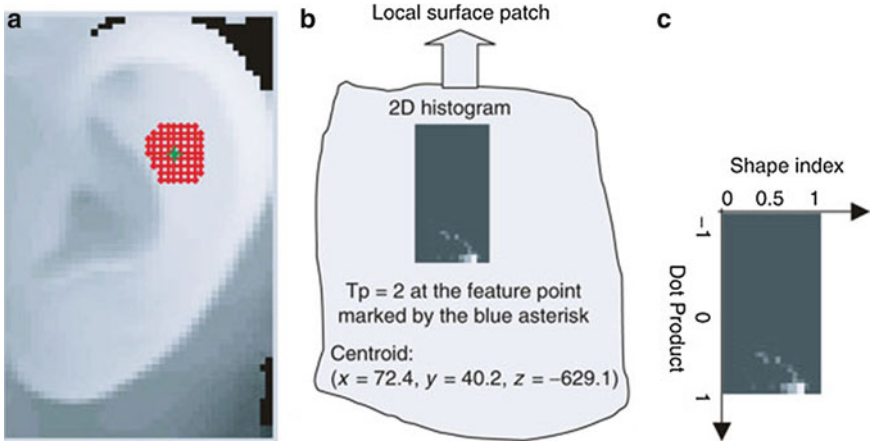


Ear Biometrics, 3D, Fig. 3 Results of ear localization on the UCR dataset. The helix and the antihelix parts are marked by *bright dots*, and the detected ear is bounded by a *rectangular box*

the 2D color images and the detected ear is bounded by the rectangular box. We observe that the ears and their helix and antihelix parts are correctly detected. This approach provides very high detection accuracy. A comparison of the three approaches shows that the first approach runs the fastest and it is simple, effective, and easy to implement. The second approach locates an ear more accurately than the first approach since the shape model is used. The third approach performs the best on both the UCR and the UND datasets, and it runs slightly slower than the other approaches.

Ear Recognition

The approach for ear detection is followed to build a database of ears that belong to different people. For ear recognition, two representations are used: the ear helix/antihelix representation obtained from the detection algorithm and a new local surface patch representation computed at



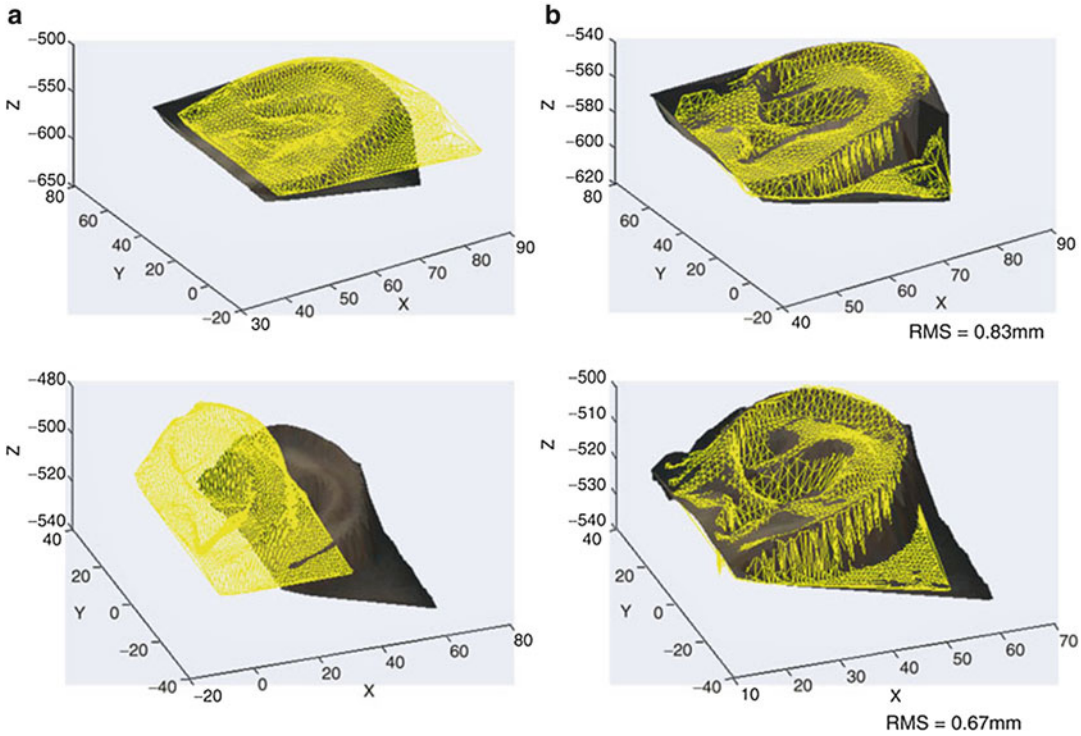
Ear Biometrics, 3D, Fig. 4 Illustration of a local surface patch (LSP). (**a**) Feature point *P* is marked by *asterisk*, and its neighbors *N* are marked by interconnected *dots*. (**b**) LSP representation includes a 2D histogram, a surface type, and centroid coordinates. (**c**) The 2D histogram is shown as a *gray* image in which the brighter areas correspond to bins with the high frequency of occurrence

feature points to estimate the initial rigid transformation between a gallery-probe pair. For the ear helix/antihelix representation, the correspondence of ear helix and antihelix parts (available from the ear detection algorithm) between a gallery-probe ear pair is established, and it is used to compute the initial rigid transformation. For the local surface patch (LSP) representation, a local surface descriptor (see Fig. 4) is characterized by a centroid, a local surface type, and a 2D histogram. The 2D histogram and surface type are used for comparison of LSPs, and the centroid is used for computing the rigid transformation. The patch encodes the geometric information of a local surface. The local surface descriptors are computed for the feature points, which are defined as either the local minimum or the local maximum of shape indexes. By comparing the local surface patches for a gallery and a probe image, the potential corresponding local surface patches are established and then filtered by geometric constraints. Based on the filtered correspondences, the initial rigid transformation is estimated. Once this transformation is obtained using either of the two representations, it is then applied to randomly selected control points of the hypothesized gallery ear in the database. A modified iterative closest point (ICP) algorithm (ICP algorithm) is run to improve the transformation, which brings a gallery ear and a probe ear into the best alignment, for every gallery-probe pair. The root mean square (RMS) registration error is used as the matching error criterion. The subject in the gallery with the minimum RMS error is declared as the recognized person in the probe.

The experiments are performed on the UCR dataset and the UND dataset.

Examples of correctly recognized gallery-probe ear pairs using the helix/antihelix representation are shown in Fig. 5. Similarly, examples of correctly recognized gallery-probe ear pairs using local surface patch representation are shown in Fig. 6. From Figs. 5 and 6, we observe that each gallery ear is well aligned with the corresponding probe ear.

The recognition results are shown in Table 1. In order to evaluate the proposed surface matching schemes, we perform experiments under two scenarios: (1) One frontal ear of a subject is in the gallery set, and another frontal ear of the same subject is in the probe set, and (2) two frontal ears of a subject are in the gallery set, and the rest of the ear images of the same subject are in the probe set. These two scenarios are denoted as ES1 and ES2, respectively. ES1 is used for testing the performance of the system to recognize ears with the same pose; ES2 is used for testing the



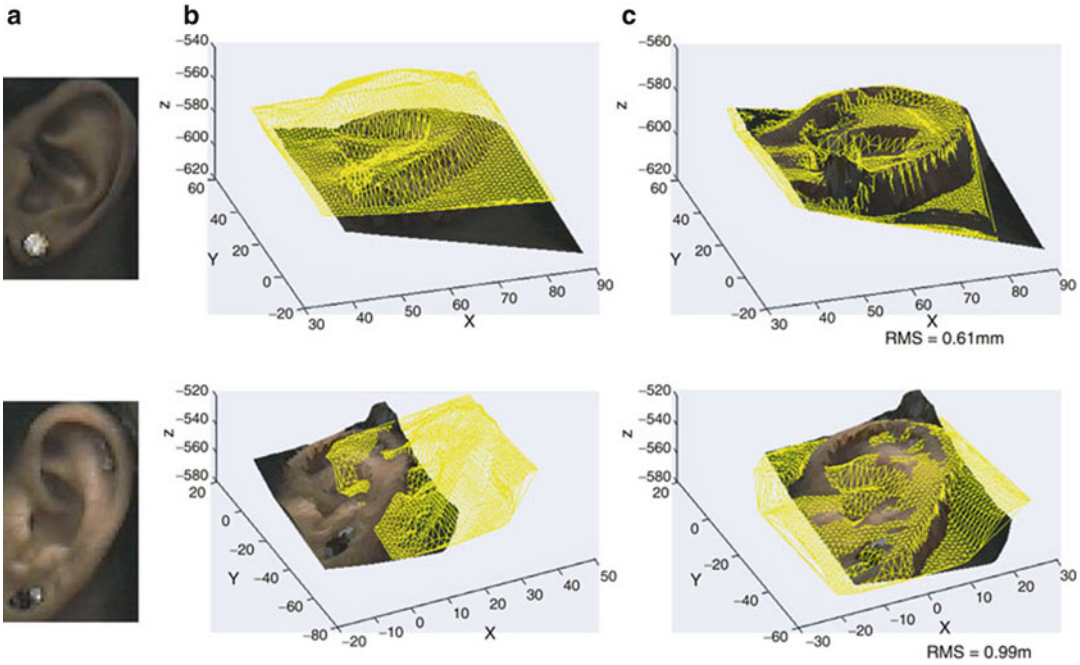
Ear Biometrics, 3D, Fig. 5 Two examples of correctly recognized gallery-probe pairs using the ear helix/antihelix representation. (**a**) Examples of probe ears with the corresponding gallery ears before alignment. (**b**) Examples of probe ears with the correctly recognized gallery ears after alignment. The gallery ear represented by the mesh is overlaid on the textured 3D probe ear. The units of x, y, and z are in millimeters (mm)

performance of the system to recognize ears with pose variations.

A comparison of the LSP representation with the spin image representation for identification and verification is given in [10]. This comparison showed that the LSP representation achieved a slightly better performance than the spin image representation.

For the identification, usually a biometrics system conducts a one-to-many comparison to establish an individual's identity. This process is computationally expensive, especially for a large database. There is a need to develop a general framework for rapid recognition of 3D ears. An approach that combines the feature embedding and support vector machine (SVM) rank learning techniques is described in [2]. It provides a sublinear time complexity on the number of models without making any assumptions about the feature distributions. The experimental results on the UCR dataset (155 subjects with 902 ear images) and the UND dataset (302 subjects with 604 ear images) containing 3D ear objects demonstrated the performance and effectiveness of the approach. The average processing times per query are 72 and 192 s, respectively, on the two datasets with the reduction by a factor of 6 compared with the sequential matching without feature embedding. With this speedup, the recognition performances on the two datasets degraded 5.8 and 2.4 %, respectively. The performance of this algorithm is scalable with the database size without sacrificing much accuracy.

The prediction of the performance of a biometric system is also an important consideration in the real-world applications. Match and nonmatch distances obtained from matching 3D ears are used to estimate their distributions. By modeling cumulative match characteristic (CMC) curve as a binomial distribution, the ear recognition



Ear Biometrics, 3D, Fig. 6 Two examples of the correctly recognized gallery-probe pairs using the LSP representation. The ears have earrings. Images in column (**a**) show color images of ears. Images in columns (**b**) and (**c**) show the probe ear with the corresponding gallery ear before the alignment and after the alignment, respectively. The gallery ears represented by the mesh are overlaid on the textured 3D probe ears. The units of x, y, and z are in millimeters (mm)

Ear Biometrics, 3D, Table 1 Recognition results on UCR and UND datasets using helix/antihelix and LSP representation

Dataset	Helix/antihelix representation					LSP representation				
	Rank-1 (%)	Rank-2 (%)	Rank-3 (%)	Rank-4 (%)	Rank-5 (%)	Rank-1 (%)	Rank-2 (%)	Rank-3 (%)	Rank-4 (%)	Rank-5 (%)
UCR ES $_1$(155, 155)	96.77	98.06	98.71	98.71	98.71	94.84	96.77	96.77	96.77	96.77
UCR ES $_2$(310, 592)	94.43	96.96	97.80	98.31	98.31	94.43	96.96	97.30	97.64	97.80
UND (302, 302)	96.03	96.69	97.35	97.68	98.01	96.36	98.01	98.34	98.34	98.34

performance can be predicted on a larger gallery [2]. The performance prediction model in [2] showed the scalability of the proposed ear biometrics system with increased database size.

Summary

Ear recognition, especially in 3D, is a relatively new area in biometrics research. The experimental results on the two large datasets show that ear biometrics has the potential to be used in the real-world applications to identify/authenticate humans by their ears. Ear biometrics can be used in both the low and high security applications and in combination with other biometrics such as face. With the decreasing cost and size of a 3D scanner and the increased performance, we believe that 3D ear biometrics will be highly useful in many real-world applications in the future. It is possible to use the infrared images of ears to overcome the problem of occlusion of the ear by hair. Recent work in acoustics allows one to (a) determine the impulse response of an ear [14]

and (b) make use of otoacoustic emissions [15] as a biometric. Thus, it is possible to combine shape-based ear recognition with the acoustic recognition of ear to develop an extremely foolproof system for recognizing a live individual.

Related Entries

▸ Face Recognition, Overview

References

1. A. Iannarelli, *Ear Identification*. Forensic Identification Series (Paramont Publishing Company, Fremont, 1989)
2. B. Bhanu, H. Chen, *Human Ear Recognition by Computer* (Springer, London, 2008)
3. M. Burge, W. Burger, *Ear biometrics*, in *Biometrics: Personal Identification in Networked Society*, ed. by A.K. Jain, R. Bolle, S. Pankanti (Kluwer Academic, Norwell, 1998)
4. M. Burge, W. Burger, Ear biometrics in computer vision. Proc. Int. Conf. Pattern Recognit. **2**, 822–826 (2000)
5. D.J. Hurley, M. Nixon, J.N. Carter, Force field energy functionals for image feature extraction. Image Vis. Comput. **20**(5-6), 311–317 (2002)
6. D. Hurley, M. Nixon, J. Carter, Force field feature extraction for ear biometrics. Comput. Vis. Image Underst. **98**(3), 491–512 (2005)
7. D. Hurley, B. Arbab-Zavar, M. Nixon, The ear as a biometric, in *Handbook of Biometrics*, ed. by A.P. Jain, A. Flynn Ross (Springer, New York, 2007)
8. K. Chang, K.W. Bowyer, S. Sarkar, B. Victor, Comparison and combination of ear and face images in appearance-based biometrics. IEEE Trans. Pattern Anal. Mach. Intell. **25**(9), 1160–1165 (2003)
9. B. Bhanu, H. Chen, Human ear recognition in 3D, in *Proceedings Workshop on Multimodal User Authentication*, Santa Barbara, 2003, pp. 91–98
10. H. Chen, B. Bhanu, Human ear recognition in 3D. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 718–737 (2007)
11. H. Chen, B. Bhanu, 3D free-form object recognition in range images using local surface patches. Pattern Recognit. Lett. **28**(10), 1252–1262 (2007)
12. P. Yan, K.W. Bowyer, Multi-biometrics 2D and 3D ear recognition, in *Proceedings of Audio and Video Based Biometric Person Authentication*, Hilton Rye Town, 2005, pp. 503–512
13. P. Yan, K.W. Bowyer, Biometric recognition using 3D ear shape. IEEE Trans. Pattern Anal. Mach. Intell. **29**(8), 1297–1308 (2007)
14. A. Akkermans, T. Kevenaar, D. Schobben, Automatic ear recognition for person identification, in *Proceedings of IEEE Workshop on Automatic Identiifcation Advanced Technologies*, Buffalo, 2005, pp. 219–223
15. M. Swabey, S.P. Beeby, A. Brown, Using otoacoustic emissions as a biometric, in *Proceedings of First International Conference on Biometric Authentication*, Hong Kong, 2004, pp. 600–606

Ear Recognition, Physical Analogies

David J. Hurley and Mark Nixon
School of Electronics and Computer Science, University of Southampton, Southampton, UK

Synonyms

Ear biometrics = Ear recognition

Definition

In the context of ear biometrics, Hurley et al. [1–3] have developed a pair of invertible linear transforms called the **force field transform** and **potential energy transform** which transforms an image into a force field by pretending that pixels have a mutual attraction proportional to their intensities and inversely to the square of the distance between them rather like Newton's law of universal gravitation. Underlying this force field, there is an associated potential energy field which in the case of an ear takes the form of a smooth surface with a number of peaks joined by ridges. The peaks correspond to potential energy wells, and to extend the analogy, the ridges correspond to potential energy channels. Since the transform also happens to be invertible, all of the original information is preserved, and since the otherwise smooth surface is modulated by these peaks and ridges, it is argued that much of the information is transferred to these features and that therefore they should make good features for recognition. An analysis of the mechanism of this algorithmic **field line feature extraction** approach leads to a more powerful method called **convergence feature extraction** based on the

divergence of force direction revealing even more features in the form of antiwells and antichannels.

Introduction

The last 10 years or so has seen increasing interest in ears as a biometrics with significant contributions from computer vision researchers [1–7], and a review is now available [12]. In this context, the force field transform was developed to be the first published approach to a working ear biometric system [1]. The transform effectively filters an ear image by convolving it with a huge inverse square kernel more than four times the size of the image, the force then being the gradient of the resulting massively smoothed image. Force field feature extraction subsequently exploits the directional properties of the force field to automatically locate ear features in the form of potential channels and wells. The force field paradigm allows us to draw upon a wealth of proven techniques from vector field calculus; for example, the divergence operator is applied to the force field direction yielding a nonlinear operator called convergence of force direction leading to the even more powerful convergence feature extraction. The extreme kernel size results in the smoothed image having a general dome shape which gives rise to brightness sensitivity issues, but it is argued by showing that the field line features are hardly distorted that this will have little overall effect and this conclusion is borne out by including brightness variation in the recognition tests. On the other hand, the dome shape leads to an automatic extraction advantage, and this is demonstrated by using deliberately poorly registered and poorly extracted images in recognition tests and then comparing the results with those for principal components analysis (PCA) under the same conditions, where the ear images have to be accurately extracted and registered for PCA to achieve comparable results. The technique is validated by achieving a recognition rate of 99.2 % on a set of 252 ear images taken from the XM2VTS face database [9]. Not only is the inherent automatic extraction advantage demonstrated, but it is also shown that it performs even more favorably against PCA under variable brightness conditions and also demonstrates its excellent noise performance by showing that noise has little effect on recognition results. Thus, the technique has been validated by achieving good ear recognition results, and in the process, a contribution has been made to the mounting evidence that the human ear has considerable biometric value.

Ear Feature Extraction

Force Field Feature Extraction

Here the force field transform and algorithmic field line feature extraction are described before introducing convergence feature extraction. The mathematical concepts used can be found in basic works on electromagnetics [8], and a more detailed description of the transform can be found in [3]. Faster computation using convolution and the fast Fourier transform (FFT) is considered and also the question of brightness sensitivity both theoretically and by demonstration.

The image is first transformed to a force field by treating the pixels as an array of mutually attracting particles that attract each other according to the product of their intensities and inversely to the square of the distances between them. Each pixel is assumed to generate a spherically symmetrical force field so that the total force $\mathbf{F}(\mathbf{r}_j)$ exerted on a pixel of unit intensity at the pixel location with position vector $\mathbf{r}_j$ by remote pixels with position vector $\mathbf{r}_i$ and pixel intensities $P(\mathbf{r}_i)$ is given by the vector summation:

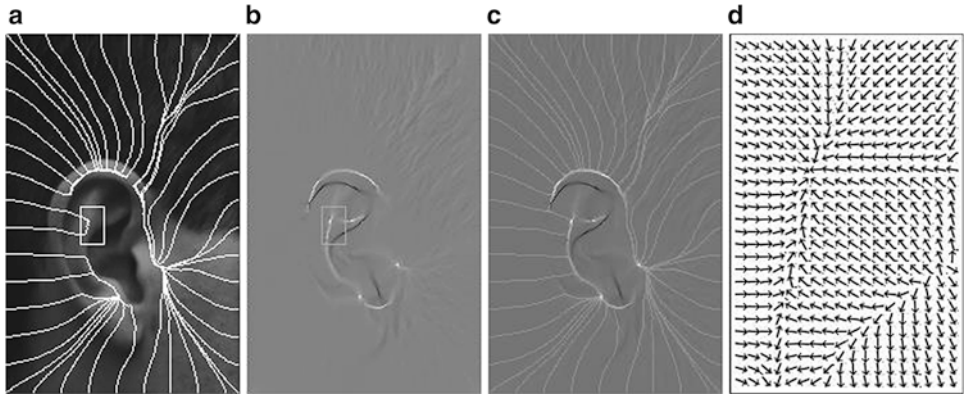
$$\mathbf{F}(\mathbf{r}_j) = \sum_i \left\{ \begin{array}{c} P(\mathbf{r}_i)\dfrac{\mathbf{r}_i - \mathbf{r}_j}{|\mathbf{r}_i - \mathbf{r}_j|^3} \forall i \neq j \\ 0 \forall i = j \end{array} \right\} \quad (1)$$

The underlying energy field $E(\mathbf{r}_j)$ is similarly described by

$$E(\mathbf{r}_j) = \sum_i \left\{ \begin{array}{c} \dfrac{P(\mathbf{r}_i)}{|\mathbf{r}_i - \mathbf{r}_j|} \forall i \neq j \\ 0 \forall i = j \end{array} \right\} \quad (2)$$

Ear Recognition, Physical Analogies, Listing 1 Force field by convolution in Mathcad

$$
\begin{aligned}
ff(pic) = \;& sr \leftarrow 2\cdot(rows(pic) - 1),\ sc \leftarrow 2\cdot(cols(pic) - 1) \\
& r \leftarrow rows(pic) - 1,\ c \leftarrow cols(pic) - 1 \\
& \text{for } rr \in 0..sr \\
& \quad \text{for } cc \in 0..sc \\
& \quad\quad usr_{rr,cc} \leftarrow \frac{(r + c\cdot j) - (rr + cc\cdot j)}{\left(\left|r + c\cdot j - (rr + cc\cdot j)\right|\right)^3} \\
& usr_{3\cdot rows(pic) - 3,3\cdot cols(pic) - 3} \leftarrow 0 \\
& pic_{3\cdot rows(pic) - 3,3\cdot cols(pic) - 3} \leftarrow 0 \\
& oup \leftarrow \sqrt{rows(pic)\cdot cols(pic)}\cdot icfft\left(\overrightarrow{(cfft(usr)\cdot cfft(pic))}\right) \\
& ff \leftarrow submatrix(oup, r, 2\cdot r, c, 2\cdot c)
\end{aligned}
$$



Ear Recognition, Physical Analogies, Fig. 1 Convergence field. (**a**) Field lines. (**b**) Convergence field. (**c**) Superimposition. (**d**) Force direction

To calculate the force and energy fields for the entire image, these calculations should be performed for every pixel, but this requires the number of applications of Eqs. 1 and 2 to be proportional to the square of the number of pixels, so for faster calculation, the process is treated as a convolution of the image with the force field corresponding to a unit value test pixel, and then invoking the convolution theorem to perform the calculation as a frequency domain multiplication, the result of which is then transformed back into the spatial domain. The force field equation for an $n-$pixel image becomes

$$
\begin{aligned}
forcefield = \sqrt{n} \times \Im^{-1}\left[\Im\left(unit\ forcefield\right)\right. \\
\left. \times \Im\left(image\right)\right]
\end{aligned}
\tag{3}
$$

where $\Im$ stands for the Fourier transform and $\Im^{-1}$ for its inverse. Listing 1 shows how to implement this in *Mathcad* in which 1**j** denotes the complex operator and **cfft** and **icfft** denote the Fourier and inverse Fourier transforms, respectively. Also, because the technique is based on a natural force field, there is the prospect of a hardware implementation in silicon by mapping the image pixels to electric charges, which would lead to very fast real-time force field calculation.

Figure 1a demonstrates field line feature extraction for an ear image where a set of 44 test pixels is arranged around the perimeter of the image and allowed to follow the field direction so that their trajectories form field lines which capture the general flow of the force field. The test pixel positions are advanced in increments

of one pixel width, and the test pixel locations are maintained as real numbers, producing a smoother trajectory than if they were constrained to occupy exact pixel grid locations. Notice the two obvious potential wells in the lower part of the field.

Convergence Feature Extraction

This analytical method came about as a result of analyzing in detail the mechanism of **field line feature extraction**. As shown in Fig. 1d, when the arrows usually used to depict a force field are replaced with unit magnitude arrows, thus modeling the directional behavior of exploratory test pixels, it becomes apparent that channels and wells arise as a result of patterns of arrows converging towards each other, at the interfaces between regions of almost uniform force direction. As this brings to mind the divergence operator of vector calculus, it was natural to investigate the nature of any relationship that might exist between channels and wells and this operator. This resulted not only in the discovery of a close correspondence between the two but also revealed extra information corresponding to the interfaces between diverging arrows, leading to a more general description of channels and wells in the form of a mathematical function in which wells and channels are revealed to be peaks and ridges, respectively, in the function value. The new function maps the force field to a scalar field, taking the force as input and returning the additive inverse of the divergence of the force direction. The function will be referred to as the **force direction convergence field** $C(\mathbf{r})$ or just **convergence** for brevity. A more formal definition is given by

$$\begin{aligned} C(r) = -\mathrm{div}\, f(r) &= -\lim_{\Delta A \to 0} \frac{\oint f(r) \cdot dI}{\Delta A} \\ &= -\nabla \cdot f(r) \\ &= -\left(\frac{\partial f_x}{\partial x} + \frac{\partial f_y}{\partial y} \right) \end{aligned} \tag{4}$$

where $f(r) = \frac{F(r)}{|F(r)|}$, ΔA is incremental area, and $d\mathbf{l}$ is its boundary outward normal. This function is real valued and takes negative values as well as positive ones where negative values correspond to force direction divergence. Listing 2 shows a particular implementation of **convergence** in Mathcad where FF represents the force field and DF is the direction field.

```
C(FF) = | DF ← FF⃗ / |FF|
        | for r ∈ 1..rows(DF) – 1
        |   for c ∈ 1..cols(DF) – 1
        |     dr ← Re(DF_{r,c}) – Re(DF_{r–1,c})
        |     dc ← Im(DF_{r,c}) – Im(DF_{r,c–1})
        |     C_{r,c} ← dr + dc
        | - C
```

Ear Recognition, Physical Analogies, Listing 2 Convergence implemented in Mathcad

It must also be stressed that convergence is nonlinear because it is based on force direction rather than force. This nonlinearity means that the operations should be performed in the order shown; this cannot be formed by taking the divergence of the force and then divide by the force magnitude. Div(grad/|grad|) $\neq$ (div grad)/|grad|. This is quite easily illustrated by a simple example using the scalar field e^x in Eq. 5:

$$\begin{Bmatrix} \text{div (grad/| grad|)} \\ \nabla \cdot \left(\frac{\nabla e^x}{|\nabla e^x|} \right) = \nabla \cdot \frac{e^x \mathbf{i}}{e^x} = \nabla \cdot \mathbf{i} = 0 \end{Bmatrix} \neq \begin{Bmatrix} \text{(div grad)/| grad|} \\ \frac{\nabla \cdot \nabla e^x}{|\nabla e^x|} = \frac{e^x}{e^x} = 1 \end{Bmatrix} \tag{5}$$

where $\mathbf{i}$ is a unit vector in the x direction. This illustrates that even though convergence looks very much like a Laplacian operator, it definitely is not.

Figure 1 shows the relationship between field lines (a) and convergence (b) by merging the two fields in (c). A small rectangular section

of the force direction field indicated by a small rectangular insert in (a) and (b) is shown magnified in (d). This shows that channels coincide with white convergence ridges and also that wells coincide with convergence peaks which appear as bright spots. Notice the extra information in the center of the convergence map that is not in the field line map. Negative convergence values representing antichannels appear as dark bands, and positive values corresponding to channels appear as white bands. The antichannels are dominated by the channels, and that the antichannels tend to lie within the confines of the channels. Notice also the correspondence between converging arrows and white ridges, and between diverging arrows and black ridges. The features detected tend to form in the center of the field due to its overall dome shape, with channels and wells tending to follow intensity ridges and peaks, whereas antichannels and antiwells tend to follow intensity troughs and hollows.

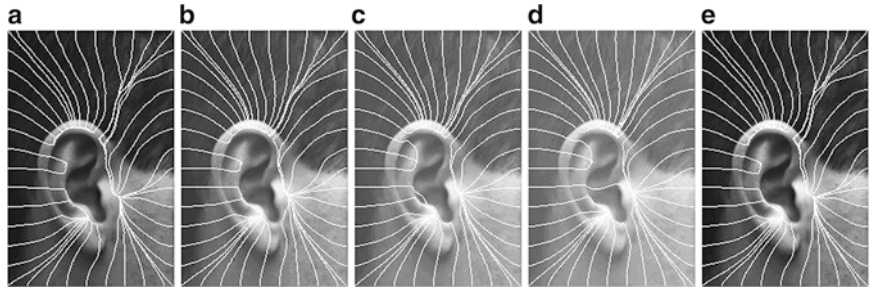
Brightness Change Analysis

Before proceeding to the next section on ear recognition, the effect of brightness change will first be analyzed by considering its effect on the energy field and then confirmed by visual experiment. Should the individual pixel intensity be scaled by a factor a and also have and an additive intensity component b, then

$$E(\mathbf{r}_j) = \sum_i \left\{ \begin{array}{c} \dfrac{aP(\mathbf{r}_i) + b}{|\mathbf{r}_i - \mathbf{r}_j|} \forall i \neq j \\ 0 \forall i = j \end{array} \right\}$$

$$= a \sum_i \left\{ \begin{array}{c} \dfrac{P(\mathbf{r}_i)}{|\mathbf{r}_i - \mathbf{r}_j|} \forall i \neq j \\ 0 \forall i = j \end{array} \right\} + \sum_i \left\{ \begin{array}{c} \dfrac{b}{|\mathbf{r}_i - \mathbf{r}_j|} \forall i \neq j \\ 0 \forall i = j \end{array} \right\} \quad (6)$$

Scaling the pixel intensity by the factor a merely scales the energy intensity by the same factor a, whereas adding an offset b is more troublesome, effectively adding a pure energy component corresponding to an image with constant pixel intensity b. The effect of the offset and scaling is shown in Fig. 2 with the channels superimposed. Scaling by a factor of 10 in (e) has no effect as expected. The original image in (a) has a mean value of 77 and a standard deviation of 47. Images (b)–(d) show the effect of progressively adding offsets of one standard deviation. At one standard deviation, the effect is hardly noticeable, and even at 3 standard deviations, the change is by no means catastrophic as the channel structure alters little. It can therefore be concluded that operational lighting variation in a controlled biometric environment will have little effect. These conclusions are borne out by the results of the corresponding recognition experiments in Table 1.



Ear Recognition, Physical Analogies, Fig. 2 Effect of additive and multiplicative brightness changes. (**a**) Original (**b**) 1 std. dev. (**c**) 2 std. devs. (**d**) 3 std. devs. (**e**) Scaled ×10

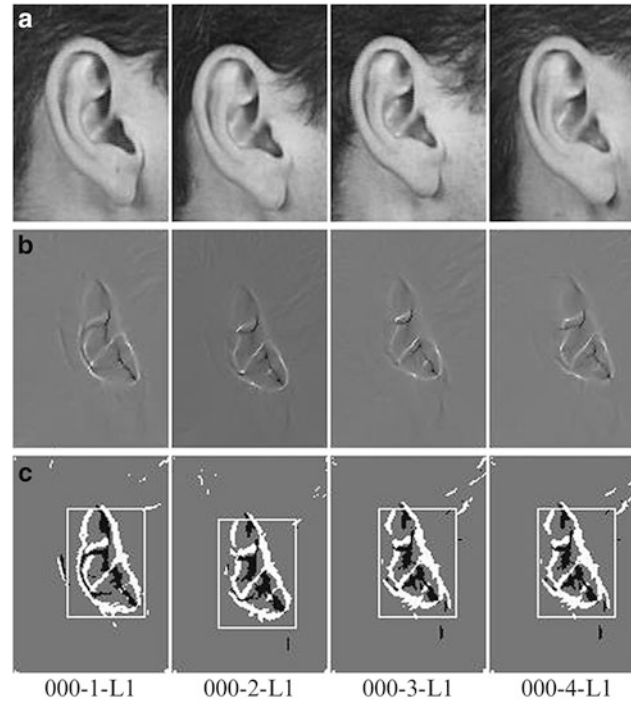
Ear Recognition, Physical Analogies, Table 1 Comparison of force field (FFE) and PCA recognition results

Image type	Method	Passes	Noise $20\log_{10}$S/N	CCR (%)	Bright. add. (std devs.)	Decidability
141 × 101 with deliberately poor extraction and registration	FFE	250/252	Nil	99.2	0	3.432
	FFE	251/252	18 dB	99.6	0	3.488
	FE	249/252	12 dB	98.8	0	3.089
	FFE	241/252	6 dB	95.6	0	1.886
	FFE	250/252	Nil	99.2	1	3.384
	FFE	247/252	Nil	98.0	2	3.137
	FFE	245/252	Nil	97.2	3	2.846
	PCA	118/189	Nil	62.4	0	1.945
111×73 with accurate extraction and registration	PCA	186/189	Nil	98.4	0	3.774
	PCA	186/189	18 dB	98.4	0	3.743
	PCA	186/189	12 dB	98.4	0	3.685
	PCA	177/189	6 dB	93.6	0	3.606
	PCA	130/189	Nil	68.8	1	1.694
	PCA	120/189	Nil	63.6	2	0.878
	PCA	118/189	Nil	62.4	3	0.476
	PCA	181/189	Nil	95.6	1 normalized	3.171
	PCA	172/189	Nil	91.0	2 normalized	1.91
	PCA	166/189	Nil	82.5	3 normalized	1.14

Ear Recognition

The technique was validated on a set of 252 ear images taken from 63 subjects selected from the XM2VTS face database [9] by multiplicative template matching of ternary thresholded convergence maps where levels less than minus one standard deviation are mapped to −1, while those greater than one standard deviation map to +1, and those remaining map to 0. A threshold level of one standard deviation was chosen experimentally resulting in the template channel thickness shown in Fig. 3c. This figure also shows a rectangular exclusion zone centered on the convergence magnitude centroid; the centroid of the convergence tends to be stable with respect to the ear features, and this approach has the added advantage of removing unwanted outliers such as bright spots caused by spectacles. The size of the rectangle was chosen as 71 × 51 pixels by adjusting its proportions to give a good fit for the majority of the convergence maps. Notice how for image 000-2, which is slightly lower than the other three, that the centroid-centered rectangle has correctly tracked the template downwards.

The inherent automatic extraction advantage was demonstrated by deliberately not accurately extracting or registering the ears in the sense that the database consists of 141 × 101 pixel images where the ears have only an average size of 111 × 73 and are only roughly located by eye in the center of these images. This can be seen clearly in Fig. 3a where there is a marked variation both in vertical and horizontal ear location and also that there is a generous margin surrounding the ears. The force field technique gives a correct classification rate (CCR) of 99.2 % on this set, whereas running PCA [10] on the same set gives a result of only 62.4 %, but when the ears are accurately extracted by cropping to the average ear size of 111 × 73, running PCA then gives a result of 98.4 %, thus demonstrating the inherent extraction advantage. The first image of the four samples from each of the 63 subjects was used in forming the PCA covariance matrix. Figure 4 shows the first 4 eigenvectors for the 111 × 73-pixel images. The effect of brightness change by addition was also tested where in the worst case where every odd image is subjected to an addition of 3 standard deviations the force field results only change by 2 %, whereas those for PCA under the same conditions fall by 36 %, or by 16 % for



Ear Recognition, Physical Analogies, Fig. 3 Feature extraction for subject 000, row (**a**), 141 × 101 ear images; row (**b**), convergence fields; row (**c**), thresholded convergence maps

Ear Recognition, Physical Analogies, Fig. 4 First 4 eigenvectors for 111 × 73 pixel images

normalized intensity PCA, thus confirming that the technique is robust under variable lighting conditions.

These results are presented in Table 1 where which also includes the decidability index after Daugman [11] which combines the mean and standard deviation of the intraclass and interclass measurement distributions giving a good single indication of the nature of the results. This index d' measures how well separated the distributions are, since recognition errors are caused by their overlap. The measure aims to give the highest scores to distributions with the widest separation between means and the smallest standard deviations. If the two means are μ_1 and μ_2 and the two standard deviations are σ_1 and σ_2 then d' is defined as

$$d' = \frac{|\mu_1 - \mu_2|}{\sqrt{\left(\sigma_1^2 + \sigma_2^2\right)/2}} \tag{7}$$

Notice that the best case index for PCA is slightly higher than the value of 3.43 obtained for the 141 × 101 images, but this could be attributed to the reduction in data set size from 252 to 189 and also to the fact that the images have been more fully extracted for PCA. Noise performance figures have also been included where noise has been modeled as additive noise with a zero mean Gaussian distribution The signal-to-noise ratios of 6, 12, and 18 dB used are calculated as $20\log_{10}(\text{S/N})$. The technique enjoys excellent noise tolerance where even for an extreme noise ratio of 6 dB the performance only falls by about 3.6 %. Interestingly at a ratio

of 18 dB, the recognition rate actually improves over the noiseless recognition rate, but this must be put down to the combination of small changes and the random nature of the noise process. For reference, the corresponding noise results for PCA under the same conditions have also been included, where PCA also performs well under noisy conditions but not quite as well as FFE at 6 dB where the fall is about 4.8 %.

Summary

In the context of ear biometrics, a linear transform has been developed that transforms an ear image, with a very powerful smoothing and without a loss of information, into a smooth dome-shaped surface whose special shape facilitates a novel form of feature extraction that extracts the essential ear signature without the need for explicit ear extraction. It has been shown that the technique is robust under variable lighting conditions both by analysis and also by experiment. Convergence feature extraction has been described, and it has been shown that it is a powerful extension to field line feature extraction. The technique has been validated by experiment where it has been shown that it compares favorably with PCA especially under variable lighting conditions. In the process, a contribution has been made to the mounting evidence in support of the recognition potential of the human ear for biometrics.

Related Entries

▸ Earprints, Forensic Evidence of
▸ Ear Biometrics

References

1. D.J. Hurley, M.S. Nixon, J.N. Carter, Force field energy functionals for image feature extraction, in *Proceedings of the 10th British Machine Vision Conference BMVC'99*, Nottingham, 1999, pp. 604–613
2. D.J. Hurley, M.S. Nixon, J.N. Carter, Force field energy functionals for image feature extraction. Image Vis. Comput. **20**, 311–317 (2002)
3. D.J. Hurley, M.S. Nixon, J.N. Carter, Force field feature extraction for ear biometrics. Comput. Vis. Image Underst. **98**(3), 491–512 (2005)
4. D.J. Hurley, B. Arbab-Zavar, M.S. Nixon, The ear as biometric, in *Handbook of Biometrics* (Springer, New York, 2008), pp. 131–150
5. P. Yan, K.W. Bowyer, Biometric recognition using three-dimensional ear shape. IEEE Trans. Pattern Anal. Mach. Intell. **29**(8), 1297–1308 (2007)
6. B. Moreno, A. Sanchez, J.F. Velez, On the Use of Outer Ear Images for Personal Identification in Security Applications, in *Proceedings of the IEEE 33rd Annual International Carnahan Conference on Security Technology*, Madrid, 5–7 Oct 1999
7. H. Chen, B. Bhanu, 3D free-form object recognition in range images using local surface patches. Pattern Recognit. Lett. **28**(10), 1252–1262 (2007)
8. M.N.O. Sadiku, *Elements of Electromagnetics*, 2nd edn. (Saunders College Publishing, New York, 1989)
9. K. Messer, J. Matas, J. Kittler, J. Luettin, G. Maitre, XM2VTSDB: the extended M2VTS database, in *Proceedings of the AVBPA'99*, Washington, DC, 1999
10. M. Turk, A. Pentland, Eigenfaces for recognition. J. Cognit. Neurosci. **3**, 71–86 (1991)
11. J. Daugman, Biometric decision landscapes. Technical report TR482, Computer Laboratory, University of Cambridge, 1999
12. A. Abaza, A. Ross, C. Hebert, M.A.F. Harrison, M.S. Nixon, A survey on ear biometrics. ACM Comput. Surv. **45**(2), 2013

Earprints, Forensic Evidence of

Christophe Champod
School of Criminal Justice – Forensic Science, University of Lausanne, Lausanne, Switzerland

Synonyms

ACE-V; Earmark(s); Earprints; Identification

Definition

Forensic evidence of earprint is the field of forensic science devoted to the collection and comparison of earmark(s) (generally left in association to a crime scene) with earprints obtained from ears of individuals of interest under controlled

condition. Anthropometric studies and empirical evidence have shown that the forms left by an ear are very discriminating and allow bringing evidence of reasonable strength regarding the identity of sources.

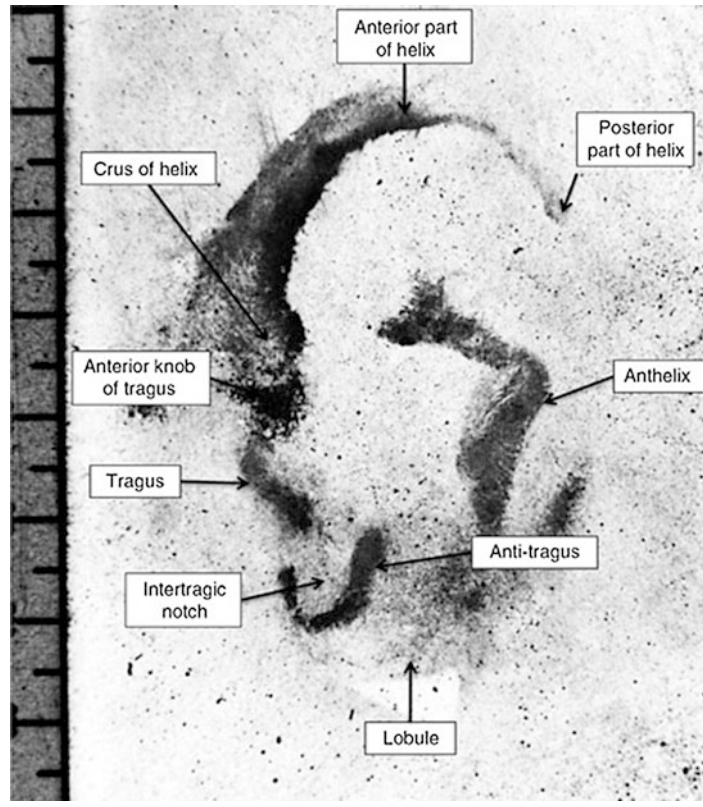
Current research aims at bringing structured data relevant to the forensic examination process and move from a field dominated by subjectively informed experience and anecdotal evidence to a field where transparent data allows an assessment of the case.

Introduction

The use of earmarks in forensic science is a consequence of the recovery of such marks during crime scene investigation. Earmarks are left on surfaces where one applies his or her ear to listen. The deposition mechanism is similar to the mechanism whereby fingermarks are deposited on surfaces when touched with bare hands. Secretions originating mainly from sebaceous glands cover the ear. When the ear is put in contact with a surface, it leaves a mark (often not readily visible), a form corresponding to the shape of the external organ applied. Such marks are often detected in conjunction with the search for latent fingermarks using the same detection techniques. The surface systematically searched for earmarks are the points of access (doors or windows), and their recovery translates a typical modus operandi for the perpetration of the offense. Marks are generally detected by applying a powdering technique on the surface. Then the mark is described, located and photographed, and preserved on an adhesive or gelatine lifter.

An example of a recovered mark is shown in Fig. 1 with indications of the typical nomenclature used to describe the features of the ear (the figure shows directly the mark, whereas these anatomical descriptions refer to the ear itself).

A useful model that helps scientists focus on their role is called the 'Investigator/Evaluator' dichotomy. In reality, scientists operate in both investigator and evaluator modes in many of the cases. Providing opinion in these two different



Earprints, Forensic Evidence of, Fig. 1 Earmark recovered from a windowpane. Anatomical features are designated with *arrows*

modes requires different mind-sets. An understanding of these differences is essential in the context of earprint analysis.

In *Investigator* mode, indeed it is the scientist's role to form a reasonable hypothesis from the observations. While attending a crime scene and recovering earmarks, the police may put forward the following investigative questions:

- How many people were involved?
- What potential set of actions may have given rise to this (these) mark(s)?
- What is the range of height of the person at the source of that (these) mark(s)?
- Using reference collections or databases, could you suggest a name to the investigation?

The scientist will form and communicate what may explain the observations based on his knowledge, experience, or through the use of databases. Generally, scientists operate in this mode before a suspect is arrested and charged with an offense. Opinions provide directions and options to the investigation, and it is accepted that some directions offered may be misleading. The problem arises when this data is not further scrutinized and used as evaluative evidence in court. In *evaluator* mode, the role of the scientist is to form a view on the weight of evidence to be assigned to the scientific findings. This is the primary role of the scientist in what may be called *post-charge* cases, i.e., cases in which a suspect has been arrested and charged. In this role, the concept of weight of evidence associated with the findings should be approached more carefully.

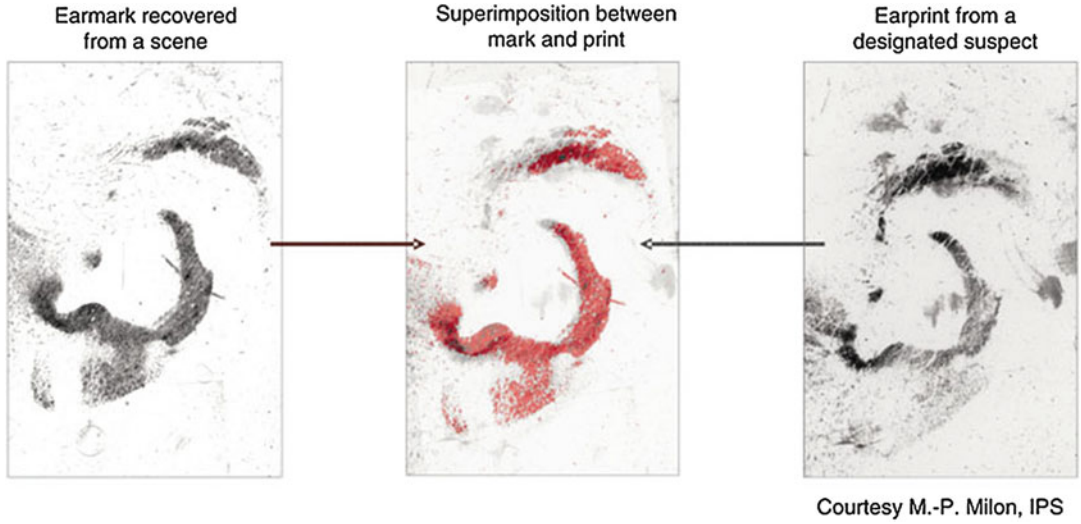
The focus here will be on this evaluative use of earprint evidence as a means to guide to the establishment of the identity of the donor of the recovered earmark(s).

Current Practice of Earmark to Earprints Comparison

The protocol used by practitioners to compare earmark(s) and earprints corresponds to the ACE-V process used in other identification fields (e.g., fingerprints) [1]. It can be summarized through the following steps:

1. The earmarks and the earprints are evaluated to assess which parts or features are visible and constitute pressure points. A specialized terminology is used to designate the anatomical parts of the ear that came into contact with the substrate (Fig. 1). Pressure points correspond to the cartilaginous parts of the ear that came into contact with the surface. The pressure on these parts is generally higher than that on the soft tissues, hence producing signs of stronger pressures on the mark as well. Also, because cartilaginous parts are less malleable than the soft tissues (such as the lobule), these pressure points tend to be more limited within-source variability.
2. Because the ear is a flexible three-dimensional object, consisting of a cartilage and a covering skin, pressure of application and rotation of the head cause differences between the successive prints from the same individual. Hence, an examination of a series of known earprints from one donor, taken under various conditions, allows the creation of an empirical model of the expected variations caused by pressure and distortion (Fig. 2). This analysis will set the tolerances that will be applied during the comparison process either to retain a potential donor as a "match" or to exclude him or her as being the contributor.
3. The earmark is compared with the earprints using overlays. The examiners look at the agreement in pressure points and measurements. The more stable features being the crus of the helix, the tragus, and the antitragus. They act as anchoring points for the overlay.
4. Differences in the comparison process are evaluated by the examiners in the light of the tolerances defined by the known effect of pressure and distortion. A decision is made as to whether any difference is significant (hence leading to an exclusion) or can be accounted for (hence leading to a "match"). The assessment of potential differences between marks and prints is left to the examiner's judgment.
5. From the quality and extensiveness of the overlay, a judgment is made as to whether

Earprints, Forensic Evidence of, Fig. 2 Earprints taken from a given individual with three degrees of pressures



Earprints, Forensic Evidence of, Fig. 3 Demonstration of the correspondence between an earmark and an earprint using the superimposition technique

the earmark and the earprints share a common origin.

6. The demonstration of the association is provided either by transparency overlays and using montages made of cut out photographs (mark and print) or using video overlays (Fig. 3).

The identification process is described mainly as a matching process – an assessment of the adequacy of superimposition between the mark and the prints – but the crucial question of the value to be given to a match is left to the examiner's judgment. In other words, when a match is declared, the assessment of the rarity of the shared features taking into account the tolerances relies on the examiner's experience.

Critical Analysis

Earmark to earprints comparison relies at the moment more on individual experience and judgment than on a structured body of research undertaken following strict scientific guidelines. The recognition process is highly subjective that exploits the extraordinary power of the human eye-brain combination.

Compared to established identification fields, such as fingerprints or handwriting comparison, the body of literature pertaining to earmarks identification is rather limited. About 60 papers have been published, a limited number in recent peer-reviewed journals. Scientific research has been mainly devoted to the study of the variability

of ear morphology based on the examination of photographs of the ear. The relevance of this body of knowledge to cases involving ear impressions found, for example, on windowpanes, is rather limited.

Most published studies on earprints have been carried out on photographs of ears and not on the earprints or earmarks [1, 2]. The limitations of such studies are obvious; there is an attempt to apply these data to the assessment of earmark to earprint comparisons for the following reasons:

- Numerous morphological features of the ear are not discernible (or cannot be classified) on earmarks.
- It is not feasible to carry out many measurements on earmarks.
- The within-source variability of features and measurements has not been fully investigated (variability, observed on marks of the same person, caused by the process of leaving and recovering marks).
- The same applies to the assessment between-persons variability (how marks from different donors can be distinguished). It is expected that the distinguishability of earmarks from different persons will be much lower than what is observed on photographs of the ear.

There is no vast empirical study exploring the chance of finding indistinguishable marks left by different individual ears. The field of earmark identification is at its infancy and would benefit from a structured program of research.

Admissibility in Court

Within the European community, there is no specific admissibility rule regarding scientific evidence (in contrast to the *Frye*/*Daubert* standard in the United States of America [3]). The principle of the judges' free evaluation of the evidence prevails. Hence, it is not surprising to see limited debate in the European jurisprudence regarding the admissibility of the earprint evidence. The current casuistic in Switzerland (known historically for the use of earprints in criminal investigations [4, 5]) gives a contrasted view between the cases where earprint has been used in court for identification (Geneva) and where the prosecution refrained from using the evidence because of its limited contribution to address the issue of identity of sources (Ticino). Earprint evidence has also been used and accepted in the courtrooms of Belgium and the Netherlands.

In the United Kindgom, two cases involving earmarks have reached the Court of Appeal. The Court of Appeal in R. v. Dallagher [6] allowed the admission of earprint evidence but received additional information that emerged more clearly since the first trial that shed some new light on the strength of the evidence. Had that evidence been available to the defense at trial, it might have reasonably affected the decision of the jury to convict and hence the conviction was quashed and a new trial was ordered [7]. The Court however ruled that earprint evidence was held admissible, leaving the duty of highlighting its limits to the adversarial system itself through a proper *voir dire* or at trial. That decision was confirmed in R. v. Mark J. Kempster [8].

In the American case State vs. Kunze [9], the Court heard some twenty experts in identification evidence and came to the conclusion that earmark identification was not a field that has gained general acceptance among peers. The Court ruled that earmark evidence cannot be accepted as scientific evidence under the Frye test. The reinvestigation of this case led to the discovery of close neighbors (close agreement between earmarks originating from different sources) among the potential donors in that case (C. Cwiklik, K.M. Sweeney, Ear Print Evidence: State of Washington v. Kunze. Personal communication from Cwiklik & Associates, 2400 Sixth Avenue South #257, Seattle, WA 98134; 2003).

Recent Research Initiatives

Early efforts toward systematic classification or matching of earprints focused on an extraction of shape features in the antihelix area and a

concept of a database based on 800 earprints from different individuals.

The field of earprint identification has been recently researched through an important initiative under funding of the European Community PF6 program FearID (http://artform.hud.ac.uk/projects/fearid/fearid.htm?PHPSESSID=9c4fd025eec23ee10262d9e226ff73d0).

They showed encouraging discriminative power but without fully addressing the issue of within-donor variation. Meijerman et al. showed the extent of changes on earprint features in terms of size and position [10]. The main source of intraindividual variation in earprints is the variation in pressure that is applied by the ear to the surface during listening. Studies in applied force while listening showed that intraindividual variation in applied force is comparatively small compared with the interindividual variation [11, 12].

Semiautomatic acquisition of earprint features was also undertaken within the FearID research program. The definition of the feature vector relied on the annotation of earprint images by skilled operators. Between-operator variations were causing a large detrimental effect on the efficiency of the system [13]. The efficiency of the developed recognition system has been tested [14]. The features are extracted from a "polyline" superimposed on the earprint by an operator. The matching is obtained using Vector Template Machine (described in http://forensic.to/fearid/VTMfinal.doc). For print to print comparisons, it was shown that for 90 % of all query searches, the best hit is in the top 0.1 % of the list. The results become less favorable (equal error rate of 9 %) for mark to print comparisons.

In addition to the described semiautomated approaches, fully automatic methods have been initially tested on a limited sample of 36 right earprints from 6 pairs of identical twins [15] using *keypoint matching* algorithms.

Some landmark research in ear biometrics [16–20] is also expected to have a drastic impact on the forensic research in earmarks in the years to come.

Related Entries

▸ Ear Biometrics, 3D
▸ Ear Recognition, Physical Analogies

References

1. C. Lugt, *van der Earprint Identification* (Elsevier Bedrijfsinformatie, Gravenhage, 2001)
2. A.V. Iannarelli, *Ear Identification* (Paramont, Fremont, 1989)
3. M.A. Berger, The Supreme Court's trilogy on the admissibility of expert testimony, in *Reference Manual on Scientific Evidence*, ed. by Federal Judicial Center (Federal Judicial Center, Washington, DC, 2000), pp. 9–38
4. F. Hirschi, Identifizierung von Ohrenabdrüken. Kriminalistik. **24**(2), 75–79 (1970)
5. F. Hirschi: Cambrioleurs internationaux convaincus à l'aide de preuves peu communes. Rev. int. police crim. **25**(239), 184–193 (1970)
6. R.*v*. Mark Dallagher, UK Court of Appeal, EWCA Crim 1903, July 25
7. Anon. Cases in brief. Archbold News. 19(8) (2003)
8. R.*v*. Mark J. Kempster, UK Court of Appeal, EWCA Crim 3555
9. State *v*. D.W. Kunze, Court of Appeals of Washington, Division 2, 97 Wash. App. 832, 988 P.2d 977
10. L. Meijerman, S. Sholl, De F. Conti, M. Giacon, C. van der Lugt, A. Drusini, et al., Exploratory study on classification and individualisation of earprints. Forensic Sci. Int. **40**, 91–99 (2004)
11. L. Meijerman, N. Nagelkerke, R. Brand, C. van der Lugt, R. van Basten, F. De Conti, Exploring the effect of occurrence of sound on force applied by the ear when listening at a surface. Forensic Sci. Med. Pathol. **1**(3), 187–192 (2005)
12. L. Meijerman, N. Nagelkerke, R. van Basten, C. van der Lugt, F. De Conti, A. Drusini, et al., Inter- and intra-individual variation in applied force when listening at a surface, and resulting variation in earprints. Med. Sci. Law. **46**(2), 141–151 (2006)
13. I.B. Alberink, A.C.C. Ruifrok, H. Kieckhoefer, Inter-operator test for anatomical annotation of earprints. J. Forensic Sci. **51**(6), 1246–1254 (2006)
14. I. Alberink, A. Ruifrok, Performance of the FearID earprint identification system. Forensic Sci. Int. **166**(2–3), 145–154 (2007)
15. L. Meijerman, A. Thean, C. van der Lugt, R. van Munster, G. van Antwerpen, G. Maat, Individualization of earprints. Forensic Sci. Med. Pathol. **2**(1), 39–49 (2006)
16. M. Choras, Ear biometrics based on geometrical method of feature extraction, in *AMDO*, Palma de Mallorca. LNCS, vol. 3179 (2004), pp. 51–61
17. K.H. Pun, Y.S. Moon, Recent advances in ear biometrics, in *Proceeding of the Sixth IEEE International*

Conference on Automatic Face and Gesture Recognition (FGR'04), Seoul, Korea 2004
18. M. Choras, Ear biometrics based on geometrical feature extraction. Electron. Lett. Comput. Vis. Image Anal. **5**(3), 84–95 (2005)
19. D.J. Hurley, M.S. Nixon, J.N.P. Carter, Force field feature extraction for ear biometrics. Comput. Vis. Image Underst. **98**, 491–512 (2005)
20. H-K. Lammi, *Ear Biometrics* (Lappeenranta University of Technology, Lappeenranta, 2005)

EEG Biometrics

Patrizio Campisi and Daria La Rocca
Section of Applied Electronics, Department of Engineering, Roma Tre University, Rome, Italy

Synonyms

Electroencephalogram-based biometrics

Definition

The analysis of electroencephalogram (EEG) has been used, for more than a century, in the medical field and also as the basis of brain computer interfaces (BCIs) and brain machine interfaces (BMI) for assistance, rehabilitative, and entertainment applications. Only recently EEG has been proposed as a biometric trait having the potentialities to allow people recognition. More specifically, an EEG recording provides a measure of the electrical activity of the brain, which reflects the summation of the synchronous activities of thousands of millions of neurons that have similar spatial orientation. In conventional scalp EEG, recordings are obtained by placing electrodes on the scalp according to the 10–20 international system and acquired either during spontaneous activity of the brain, like a resting state with open or closed eyes, or in the presence of specific stimuli or events. Scalp EEG activity shows oscillations at a variety of frequencies, mainly in the range $[1, 40]$ Hz. Several of these oscillations show characteristic frequency content and spatial distributions, associated to different states of brain functioning, that can be investigated as potential distinctive traits for the purpose of user recognition.

Introduction

In the last decade, an always growing interest in the use of biological signals for the purpose of automatic user recognition is being witnessed. Within this framework, among the possible acquirable biological signals, those sensing the brain activity have recently attracted the attention of the research community due to the evidence that they carry distinctive information about the individual identity. Specifically, brain activity can be registered either by measuring the blood flow or by measuring the neuron activity. To the first category belong approaches like functional magnetic resonance imaging (fMRI), which measures the concentration of oxygenated and deoxygenated hemoglobin in response to magnetic fields; the near-infrared spectroscopy (NIRS), which measures the concentration of oxygenated and deoxygenated hemoglobin by means of the reflection of infrared light by the brain cortex through the skull; and the positron emission tomography (PET), which measures neuron metabolism through the injection of a radioactive substance in the subject. To the second category belong approaches like magnetoencephalography (MEG), which is sensitive to the small magnetic fields induced by the electric currents in the brain, and electroencephalography, which is sensitive to the electrical field generated by the electric currents in the brain.

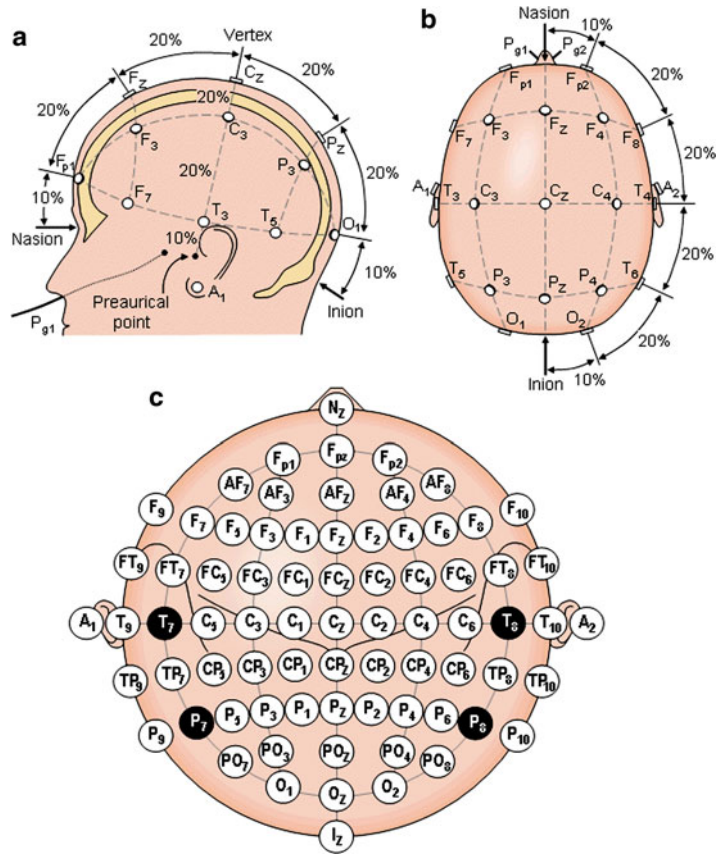
Specifically, EEG recordings are acquired with portable and relatively inexpensive devices when compared to the other brain imaging techniques. They measure the voltage fluctuation on the scalp surface resulting from the electric field generated by the firing of collections of pyramidal neurons of the cortex. For instance, EEG oscillations can describe the brain response to either external or internal stimuli which generate the so-called event-related potentials

(ERPs). The EEG amplitude of a normal subject in the awake state, recorded with scalp electrodes, is in the range of $[10, 100]\,\mu V$. The way the brain regions and structures are organized and coordinated during specific cognitive functions or mental states is considered to be a typical feature of each subject, due to both morphological and anatomical traits, and functional plasticity traits.

While conventional biometric systems rely on the use of either physiological or behavioral characteristics, that is, on some biological characteristic the user "possesses" or on the "way the individual behaves," respectively, the systems we deal about hereafter are based on the "way the individual thinks" as a distinctive characteristic for automatic user recognition, thus focusing on the use of EEG signals, describing the electrical activity of the brain, as a biometric trait of an individual [1, 2].

EEG Measurement

EEG signals can be acquired with devices which consist of a set of amplifiers, a multichannel analog-to-digital converter, and a set of electrodes, placed on the scalp, which sense the electrical activity of the brain. The electrodes can be either needle electrodes, which are very invasive, passive electrodes, which need conductive gel to reduce the electrode-skin impendence, or active electrodes, not requiring any paste. Electrodes positioning is made according to the conventional electrodes setting, namely, the 10–20 international system, recommended by the International Federation of Societies for Electroencephalography and Clinical Neurophysiology. This recommendation is shown in Fig. 1a, b for systems using 21 electrodes. In Fig. 1c an extension of the 10–20



EEG Biometrics, Fig. 1 The 10–20 international system seen from left (**a**) and above the head (**b**). The letters *F*, *T*, *C*, *P*, and *O* stand for frontal, temporal, central, parietal, and occipital lobes. Even numbers identify electrodes on the right hemisphere, odd numbers are those on the left hemisphere, and "z" (zero) refers to electrodes placed on the midline (Jaakko Malmivuo and Robert Plonsey, Bioelectromagnetism, Oxford University Press, 1995, WEB version)

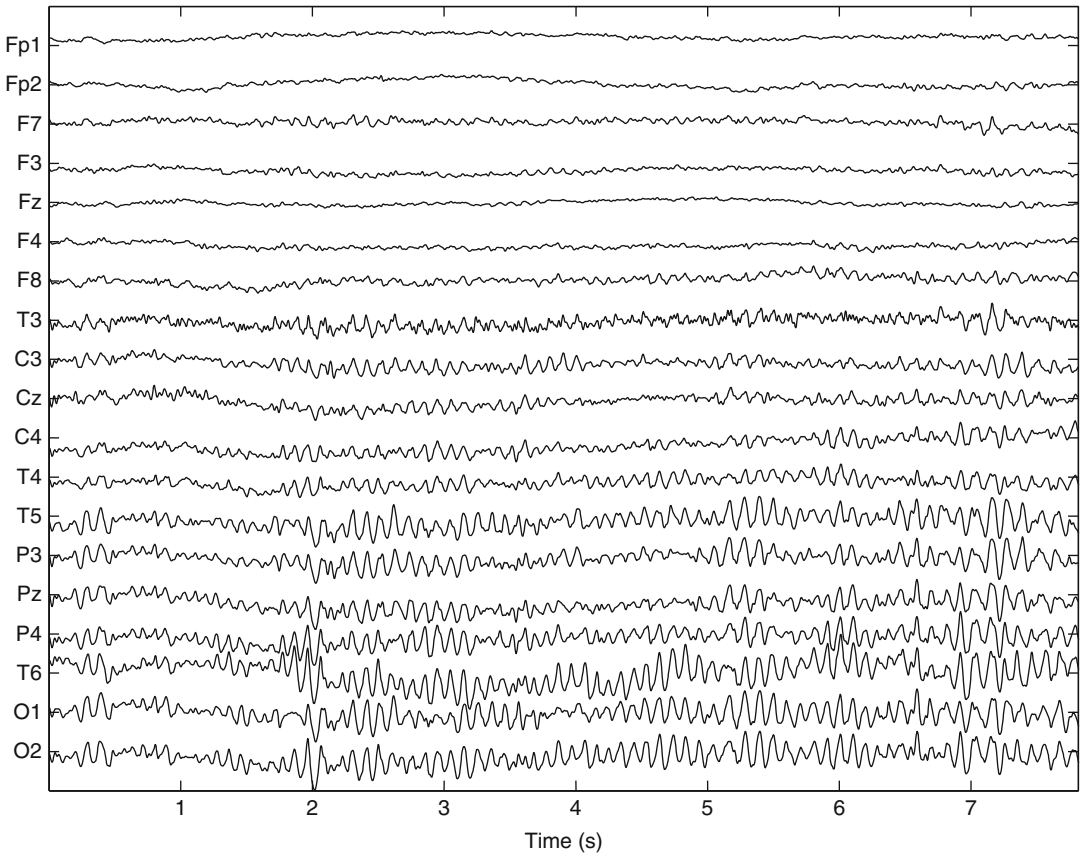
international system to 75 electrodes, which allows a higher spatial resolution, is shown.

The EEG signals show different features according to the different acquisition protocols that are employed in the recording session. In fact the collection of EEG signals can be performed either in a situation of spontaneous activity of the brain like a resting state with either open or closed eyes or in the presence of specific stimuli or events, like visual, auditory, or tactile stimuli; the execution of real or imagined body movements; and also the performance of imagined speech. Moreover EEG can be acquired while a subject is stimulated by natural stimuli like music, speech, or video. Therefore the brain response to different stimuli produces signals which can differ significantly being generated in different areas of the brain, showing different frequency components and amplitude.

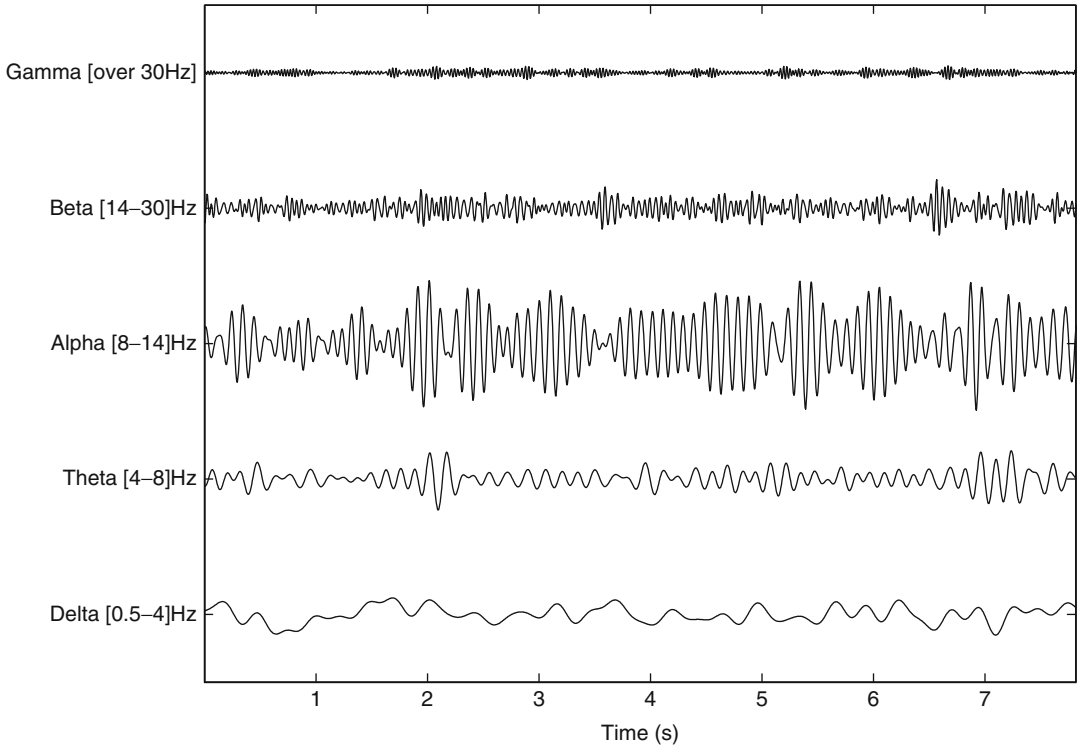
The most relevant cerebral activities fall in the range of $[0.5, 40]$ Hz. The amplitude of the EEG signals is up to about $100\,\mu$V when measured on the scalp and about 1–2 mV when measured on the cortex. An example of the signals acquired using a 19-channel amplifier with the electrodes positioned according to the 10–20 international system is given in Fig. 2.

Roughly speaking five main brain rhythms can be identified, each associated with a specific bandwidth:

- *Delta waves* (δ) $[0.5, 4]$ Hz primarily associated with deep sleep and loss of body awareness. They may be present in the waking state.
- *Theta waves* (θ) $[4, 8]$ Hz associated with deep meditation and creative inspiration, and they may also appear in dreaming sleep (REM stage).



EEG Biometrics, Fig. 2 Example of an electroencephalogram acquired using a 19-channel system using a "rest state with closed eyes" protocol



EEG Biometrics, Fig. 3 Examples of delta, theta, alpha, beta, and gamma waves acquired through the channel O2 using a "rest state with closed eyes" protocol

- *Alpha waves* (α) [8, 13] Hz indicating either a relaxed awareness state without any attention or concentration. They are reduced by anxiety, mental concentration or attention.
- *Beta waves* (β) [13, 30] Hz usually associated to an alert state, active thinking, and attention.
- *Gamma waves* (γ) over 30 Hz present low amplitude; they can be used as indicators of event brain activity synchronization.

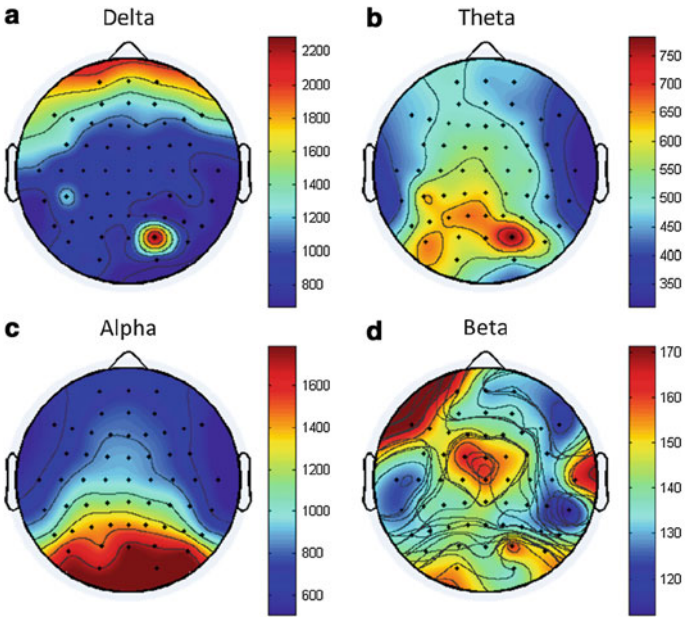
Some examples for each of the aforementioned brain rhythms are given in Fig. 3. In Fig. 4 the topographic maps related to the main brain rhythms during resting with closed eyes are displayed in false colors. The strong parieto-occipital α activity can be observed in the related map. Also the spatial distributions on the scalp of the other rhythms showing smaller amplitude during rest (δ, β, θ) are shown beside.

EEG-Based User Recognition

An EEG-based biometric recognition system, as a generic biometric- based system, is composed of an acquisition module that senses the EEG signals, a preprocessing block that performs noise and artifact removal, a feature extraction module that extracts the representative elements of the EEG signals, and a matching block producing a score that is used to provide a ranking of the most probable users or, when feeding a decision module, to provide a decision about the user's claimed identity.

EEG as Biometrics

With respect to more mature biometrics like fingerprints, iris, and face, EEG signals present some peculiarities which are beneficial for the design of secure and privacy compliant biometric systems. In fact EEG, being the result of ionic



EEG Biometrics, Fig. 4 Topographic maps of rhythms. Each map shows in false colors the spatial distribution on the scalp surface of the related EEG rhythm's mean power, for a test subject. Maps for rhythms delta (**a**), theta (**b**), alpha (**c**), and beta (**d**) are reported. Each circle represents the top view of a head, where the highest point is the nasion while the lowest is the inion

current flows within the neurons of the brain, are not exposed like face, iris, and fingerprints; therefore they cannot be captured at a distance or they cannot be acquired at a later time, like it may happen for latent fingerprints. Therefore, EEG signals are "secret" by their nature, and they give to a biometric-based recognition system a higher level of privacy compliance than other biometrics. Nevertheless, once the signals are acquired, they can reveal personal health information, like it happens for face, iris, and fingerprints. Therefore privacy protection mechanisms need to be put in place when handling such biometrics. Furthermore, EEG-based biometric systems are inherently robust against sensor spoofing. In fact, following the previous argumentations, conventional biometrics like face, iris, and fingerprints can be easily acquired by an attacker, synthetically generated at a later time, and fed to the acquisition sensors. This is not feasible when using EEG signals since an attacker should be able to acquire them covertly and feed them to the sensors, which is not possible at the present state of technological development. This also inherently solves the problem of liveness detection without the need to resort to specifically designed sensors. Moreover, EEG biometrics has a higher level of universality than conventional biometrics. Furthermore, since EEG signals present a good time resolution, they are among those biometric that allow continuous verification, so that the presence of the same individual can be constantly and transparently monitored by analyzing the person's spontaneous brain activity or the response to cognitive stimuli, thus avoiding the possibility of substitution as possible in a one-time login system. On the other hand, the use of EEG signals within the framework of biometric recognition presents some drawbacks, being the acquisition devices more expensive than the ones used for classical biometrics and having the system a high level of intrusiveness which limits the user convenience and its level of acceptability. Moreover, neurological studies have demonstrated that the EEG can be considered a genotypic characteristic which limits its uniqueness.

EEG Biometrics: State of the Art

EEG signals are usually contaminated by noise and artifacts which can be both endogenous and exogenous events with respect to cerebral activity. In fact, being the brain continuously and spontaneously active, there is a background noise, superimposed to the signals representing

the synchronous firing of specific collections of neurons which respond accordingly to the cognitive stimulus. Moreover, biological artifacts, like the ones related to eye movements, to hearth beat, and to muscle activity, can occur. Therefore a preprocessing stage, consisting, for example, in adaptive filtering, principal component analysis (PCA), blind source separation (BSS), etc., is always needed for the purpose of noise and artifact removal, before performing feature extraction.

EEG as biometrics was first introduced in [3] where a "closed eyes in resting conditions" protocol was employed to acquire data using the O2 channel. The α rhythm was isolated and then modeled using autoregressive (AR) modeling with order ranging from 8 to 12. A Kohenen linear vector quantizer was employed. The tests performed was aimed to verify four *authorized* users against a single class of *non-authorized* users. The performance expressed in terms of genuine authentication rate (GAR) ranged between 72 and 84 %. In [4] the EEG activity was recorded from 40 subjects while resting with open eyes and with closed eyes. Although eight sensors were employed for the acquisition, only the signals acquired using the channel P4 were used in the modelization. In detail, after preprocessing aimed at removing noise and other undesirable components, AR modeling of order ranging from 3 to 21 was employed. A discriminant analysis was performed, and GAR ranging from 49 to 82 % depending on the AR model order was obtained. In [5] VEP stimuli consisting in showing black and white drawings of common objects were used during the recording of the EEG signals. A database of 102 people was used, and signals from 61 channels were acquired. After having filtered the signals with a 25–56 Hz pass band filter, the MUSIC algorithm was used to estimate, for each signal, both the dominant frequency and the power content. These estimates for all 61 channels were used as the feature vector. An Elman neural network was employed as classifier. A GAR of 98.12 % was reached. In [6] imagined related tasks such as imagination of left-hand movements and of right-hand movements and the generation of words beginning with the same random letter were considered to generate EEG signals. The employed database was constituted by acquiring eight channels for nine users. Specifically the centro-parietal channels C3, Cz, C4, CP1, CP2, P3, Pz, and P4 were used. The signals were preprocessed by retaining the band 8–30 Hz. A Gaussian Mixture Model together with maximum a posteriori (MAP) adaptation were employed. Different experiments were performed, and a half total error rate HTER (HTER = (FAR+FRR)/2) ranging from 8.4 and 42.16 % was achieved for imagined motion, whereas for word generation a HTER = 12.1 % was achieved. In [7] a closed eyes resting condition was used to acquire EEG signals from 51 subjects employing 2 forehead electrodes (FP1 and FP2). The feature vector was built by concatenating several features: the AR coefficients up to order 100, the DFT coefficients in the band 1–40 Hz, the mutual information (MI), the coherence (Coh.), and the cross-correlation between the two acquired signals. Discriminant analysis with four different functions was used, and the best achievable result was an equal error rate (EER) equal to 3.4 %. In [8] data were acquired while seven subjects performed real motion-related tasks. Seventeen channels have been employed and clustered in five groups according to their physical position. Then, independent component analysis was performed in each region, thus selecting the most energetic component for each region as a feature. AR modeling, with order equal to seven, was then performed on each of the selected components, thus obtaining the feature vector. A naive Bayes classifier was used and a HTER = 4.1 % was achieved. In [9] two different datasets were used: one for VEP, collected showing black and white images to 120 people while recording the EEG using 64 channels, and the other one for imagined speech, where 6 volunteers imagined speaking the two syllables /ba/ and /ku/, and the recording was performed using 128 sensor channels. The so obtained signals were preprocessed in order to remove the artifacts, and then autoregressive (AR) modeling for each signal acquired by the sensor net was performed. A support vector machine (SVM) classifier was employed for both acquisition protocols, thus

EEG Biometrics, Table 1 Overview of state-of-the-art contributions using EEG signals as a biometrics

Paper	Protocol	Database	Channels	Features	Classifier	Performance
Poulos et al. [3] '99	Closed eyes	4	1 (O2)	AR (8th–12ve)	Kohonen's LVQ	GAR = 72–84 %
Paranjape et al. [4] '01	Closed/Open eyes	40	1 (P4)	AR (3rd–21st)	Discriminant Anal.	GAR = 49–82,%
Palaniappan and Mandic [5] '07	VEP	102	61	MUSIC	Elman NN	GAR = 98.12 %
Marcel and Millán [6] '07	Imagined movement	9	8	GMM	MAP model adaptation	HTER = 8.4–42.6 %
	Word generation	9	8	GMM	MAP model adaptation	HTER = 12.1 %
Riera et al. [7] '08	Closed eyes	51	2 (FP1, FP2)	AR (100th) & DFT MI & Coh. & CrossCorr.	Discriminant Anal.	EER = 3.4 %
He and Wang [8] '10	Motion related tasks	7	17	AR (7th) on ICA	Naive Bayes Classifier	HTER = 4.1 %
Brigham and	Imagined Speech	6	128	AR (2nd)	Support Vect. Mach.	GAR = 99.76 %
Vijaya Kumar [9] '10	VEP	120	64	AR (4th)	Support Vect. Mach.	GAR = 98.96 %
Su et al. [10] '10	"Water/coffee"	40	1 (FP1)	AR (19th) & PDS	k-NN	GAR = 97.5 %
Campisi et al. [11] '11	Closed eyes	48	3 (T7,Cz,T8)	AR (6th)	Polynomial regression	GAR = 96.98 %
La Rocca et al. [12] '12	Closed eyes	45	2, 3, 5	AR (6th)	Polynomial regression Fusion of bands	GAR = 98.73 %

achieving a GAR = 99.76 % for the case of imagined speech with a 2nd- order AR model, whereas a GAR = 98.96 % was obtained using a 4th- order AR for the VEP case. In [10] the influence of the diet and circadian effects on the identification was investigated by using a protocol where EEG signals acquired by the FP1 electrode were recorded before and after coffee assumption. A database of 40 subjects was collected. A feature vector composed of AR coefficients estimated on the whole signal plus the power spectral density (PDS) in the frequency range of [8, 32]Hz was considered. Classification performed by using K-NN along with feature reduction using Fisher's linear discriminant analysis (FDA) gave a recognition accuracy of 97.5 %. In [11] a database of 48 subjects in a closed eyes resting state was acquired using a 56-channel acquisition system. However only triplets of electrodes have been used in the analysis. A six-order AR model has been estimated for each channel and a polynomial regression-based classification has been employed, obtaining a GAR of 96.08 % when using the triplet T7, Cz, T8. In [12] the same acquisition protocol and modeling in [11] has been employed. However a more extensive analysis on the sensors' optimal number and their spatial localization has been performed by considering configurations involving two, three, and five sensors respectively. Also fusion among the different subbands has been analyzed. GAR of almost 99 % has been achieved.

A summary of the aforementioned contributions is given in Table 1 where details about the protocol used to acquire the EEG signals, the dimension of the database analyzed, the number of channels employed to acquire the signals, the extracted features, the considered classifier, and the achieved performance are given.

Research Directions

The use of EEG signals as biometrics is bearer of both a new paradigm and new challenges in the scenario of automatic user recognition. Differently from physiological-based biometric systems, which rely on physical attributes the user possess, and from behavioral-based biometric systems, which rely on how the user behaves, the resort to EEG signals paves the road towards the use of the mental signature of a user in a cognitive process as a mean for recognition. Despite some preliminary studies, which have demonstrated the feasibility of using EEG signals as biometrics, many questions remain open and need a more deep and systematic investigation. Issues such as the level of user discriminability that EEG signals can guarantee, the EEG permanence in time (see [13] for a preliminary study), and their relationship with the acquisition protocol need to be investigated. More specifically, the appropriate stimulation that elicits the user's most discriminant mental signature needs to be properly designed. Furthermore, the electrodes configuration both in number and location has to be optimized, accordingly to the employed stimulus, in order not to affect significantly the user convenience, still guaranteeing the maximum performance. Furthermore, the EEG stability in time for the same user, i.e., the intraclass variability, and its discriminative power for different users, i.e., the interclass variability, are not fully understood yet. Although the bases for the use of EEG for user automatic recognition have already been posed, a deep and systematic investigation on the aforementioned issues needs to be carried out in order to deploy in the future a highly secure, accurate, and convenient EEG-based recognition system in everyday life.

Related Entries

- ▸ Biometric Template Binarization
- ▸ Biometric Verification/Identification/ Authentication/Recognition: The Terminology

References

1. P. Campisi, D. La Rocca, G. Scarano, EEG for automatic person recognition. Computer **45**(7), 87–89 (2012)
2. P. Campisi, D. La Rocca, Brain waves for automatic biometric based user recognition. IEEE Tran. Inf. Forensics Secur. **9**(5), (2014)
3. M. Poulos, M. Rangoussi, V. Chrissikopoulos, A. Evangelou, Person identification based on parametric processing of the EEG, in *The 6th IEEE International Conference on Electronics, Circuits and Systems (ICECS'99)*, Pafos, Greece, 1999, pp. 283–286
4. R. Paranjape, J. Mahovsky, L. Benedicenti, Z. Koles, The electroencephalogram as a biometric, in *Canadian Conference on Electrical and Computer Engineering*, Toronto, Canada, 2001, pp. 1363–1366
5. R. Palaniappan, D. Mandic, Biometrics from brain electrical activity: a machine learning approach. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 738–742 (2007)
6. S. Marcel, J.R. Millan, Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 743–748 (2007)
7. A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, G. Ruffini, Unobtrusive biometric system based on electroencephalogram analysis. EURASIP Journal on Advances in Signal Processing 2008, 2008.
8. C. He, Z.J. Wang, An independent component analysis (ICA) based approach for EEG person authentication. in *3rd International Conference on Bioinformatics and Biomedical Engineering (ICBBE'09)*, Beijing, China, 2010
9. K. Brigham, B.V. Kumar, Subject identification from electroencephalogram (EEG) signals during imagined speech, in *Proceedings of the IEEE Fourth International Conference on Biometrics: Theory, Applications and Systems (BTAS'10)*, Washington, DC, 2010
10. F. Su, L. Xia, A. Cai, Y. Wu, J. Ma, EEG-based personal identification: from proof-of-concept to a practical system, in *20th International Conference on Pattern Recognition (ICPR 2010)*, Istanbul, Turkey, 2010, pp. 3728–3731
11. P. Campisi, G. Scarano, F. Babiloni, F. De Vico Fallani, S. Colonnese, E. Maiorana, L. Forastiere, Brain waves based user recognition using the "eyes closed resting conditions" protocol, in *IEEE International Workshop on Information Forensics and Security (WIFS'11)*, Iguacu Falls, Brazil, 2011
12. D. La Rocca, P. Campisi, G. Scarano, EEG biometrics for individual recognition in resting state with closed eyes, in *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, 2012
13. D. La Rocca, P. Campisi, G. Scarano, On the repeatability of EEG features in a biometric recognition framework using a resting state protocol, in *BIOSIGNALS*, Barcelona, Spain, 2013

Embedded Systems

Naohisa Komatsu[1] and Manabu Nakano[2]
[1]Waseda University, Shinjuku-ku, Tokyo, Japan
[2]Information-Technology Promotion Agency (IPA), Bunkyo-ku, Tokyo, Japan

Synonyms

Embedded processor; Embedded software

Definition

Embedded systems [1, 2] are computer systems that are embedded in various parts of equipment to control them. There is also another definition: embedded systems are integrated systems that are combined with equipment. Examples of equipment to which embedded technologies are applied include electrical household appliances and electrical equipment, PC peripheral equipment, office automation equipment, communications equipment, network facilities, medical equipment, and robots. Embedded systems are rapidly spreading wide to include social life, but there are some problems. The greatest challenge is to keep or improve the quality of design and reliability as the systems get large and complex. Biometric authentication functions have been already embedded in smart cards and cellular phones. Embedded authentication functions are applied to the driving system and personal comfort equipment at home; system security and usability are other important aspects to be studied.

Profile of Embedded System

Those devices that are traditionally controlled by hardware-like logic have advanced significantly with the use of super micro computers and their control software since the 1980s. As a result, any complicated embedded system can be created, even in a small space and at low cost: every device, such as home appliances, mobile phones, vehicles, and industrial robots, is being popularized as an "embedded system." Biometric products are also considered "embedded systems" and will be embedded in a variety of devices such as vehicles, mobile phones, etc, in the near future. In addition, because of advanced IT technology, it is becoming easy to include communication functions; "embedded systems" are evolving as one of the infrastructural devices in ubiquitous networks, allowing us to utilize networks anytime and anywhere.

Add-on systems are defined as hardware systems in which certain software is installed, upon procurement from its manufacturer. In biometric authentication, the software is referred to as the authentication software, and enables us to characterize biometric data and cross-check biometric data between and the driver, which controls the sensor for biometric authentication. As the devices integrated with such software are commonly employed in biometric authentication products, most often, biometric authentication is done by add-on systems.

The product/system for biometric authentication can generally be classified into the following four categories, depending on how the biometric information sensor and the software that can serve authentication and/or the biometric data memory, which stores individual biometric data, are integrated with the entity (i.e., the system) that implements their original objectives upon procurement.

All-in-One

All the three – the biometric information sensor, the biometric authentication software, and the biometric data memory – are integrated with the entity (i.e., the system). The stand-alone laptop type computer with finger print authentication sensor, a door security device, and a car with finger print authentication are in the family of such biometric authentication products. The mobile telephone with finger print authentication, which is popular in Japan, is also an all-in-one biometric authentication product.

Biometric-Information-Data-Separation Method

The biometric information sensor and the biometric authentication software are integrated with the entity, but the biometric data memory is

located separately. The biometric memory may be a handheld type of memory medium such as a smartcard and/or the server in a server-client system. The method of using a smartcard as a biometric data memory is referred to as STOC (store on card) authentication method.

Authentication-Sequestration Method

In this method, only the biometric authentication sensor is integrated with the entity (i.e., the system), but the biometric authentication software and the biometric data memory are located separately. That is, the biometric data fed by the biometric authentication sensor is transferred to a different system/device where biometric data are registered and cross-checked. As for the different system/device, a smartcard and/or the server, and part of a server-client system are included. As the smartcard itself is a device, the authentication software and/or individual data memory with the authentication method is exclusively referred to as MOC (match on card) authentication method.

Authentication-Unit

The biometric authentication sensor, biometric authentication software, and biometric data memory form a unit. It may be configured after providing the SIer and third party (ies) biometric authentication mechanism. This can provide vendors and SIer with the most simple and manageable biometric authentication.

Difference Between Embedded System and General System

What if we do not conduct certain security measures on the general computer systems connected to a network? They will be infected with virus within a short period of time and/or they will be easily attacked by malicious persons. To avoid that, it is necessary to conduct certain security measures, utilizing anti-virus software, firewall, 'etc., and in case of some vulnerability in software, we can maintain security by downloading and applying security patches in general systems. However, in an "embedded system," it is harder to address the said measures because of the constraints in utilizing their resources. In addition, there are the "embedded system"-specific issues such as side-channel attack and reverse engineering.

It is expected that along with advancement, such security issues looming up in the world of computer systems will be a great threat to the "embedded system" in the years to come. There are only some accidents relevant to the "embedded system" that have been reported and it is not likely that they will happen frequently hereafter. It is ideal to construct the lifecycle of the "embedded system" in four different phases: planning, development, operation, and discarding, to implement sufficient security measures by both developers and users (Fig. 1).

Instances of Embedded System in IC Card

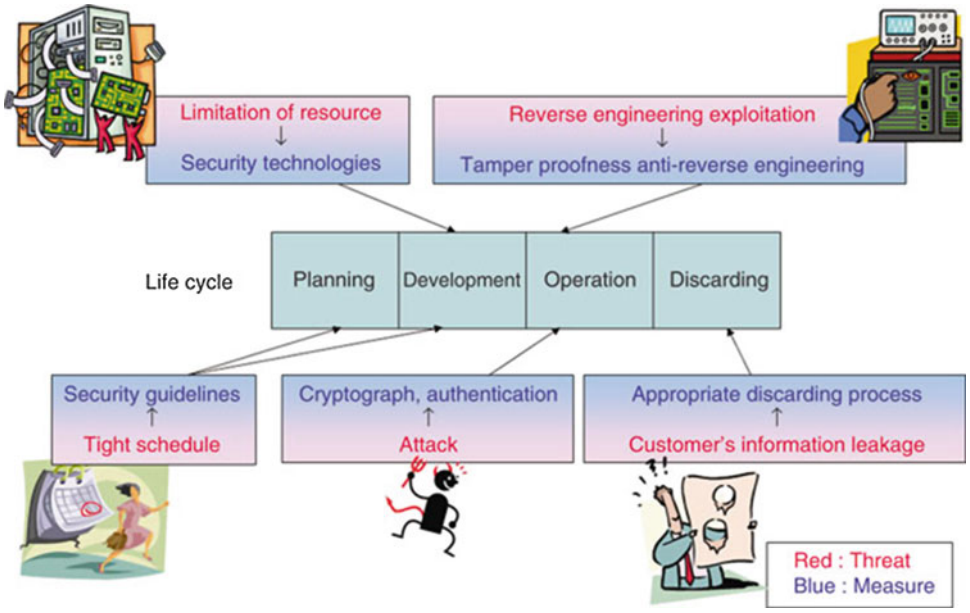
In this section, the essay introduces the IC card as one of the instances of specific embedded systems. Generally, it can be assumed that the "manufacturer," "issuer," and "holder" will be involved in the lifecycle of the IC card from its planning to discarding phases (Fig. 2).

There exist different threats in each phase of the lifecycle:

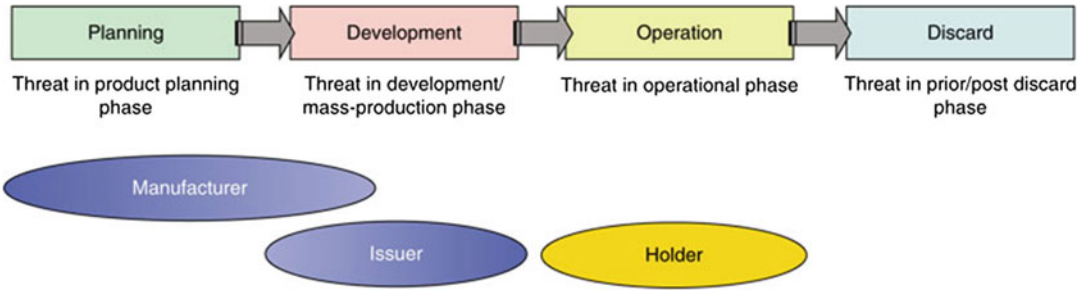
To avoid these problems, it is necessary to adopt certain security measures such as encryption of the design document, periodic logical verification, and regulation of prior/post disposal, etc, for the respective holders' further security. For effective security, all the measures have to be employed to work synergically.

Instances in Biometrics

Figure 3 shows the vulnerabilities of a biometric authentication system [3, 4], and the vulnerabilities [5] are explained in Tables 1 and 2. Vulnerabilities can be classified into two types:

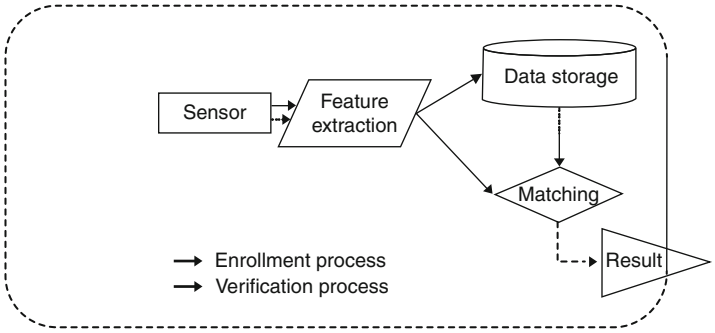


Embedded Systems, Fig. 1 Potential problems & measures



Embedded Systems, Fig. 2 Lifecycle of IC card

Embedded Systems, Fig. 3 Vulnerabilities in biometric systems



Embedded Systems, Table 1 Biometric-specific vulnerabilities

Name of vulnerability	Definitions
Familiarity/Proficiency	Certain familiarity/proficiency is necessary upon utilizing biometric system
Acceptability	Some users are still reluctant to use biometric system
FAR (False Accept Rate)	Accidental occurrence of FAR
FRR (False Reject Rate)	Accidental occurrence of FRR
Unavailability	There are some users who cannot be authenticated biologically or are those for which biometric data cannot be obtainable from
User Status	Data granularity will vary depending on user's physical status
Entering Environment (Minutia Angle, etc.)	Data granularity will vary depending on entering environment, such as minutia angle, etc.
Wolf	FAR occurs with high probability due to Wolf
Lamb	FAR occurs with high probability due to Lamb
Goat	FRR occurs with high probability due to Goat
Authentication Parameter	Inadequate matching performance relevant to configuration of authentication parameter
Falsified biometric Information	Physically generation of falsified biometric information
Publication	Anyone else can acquire user's biometric information
Assumption	Assumable biometric information from templates/matching results
Extent	Number of attempts available to biometric information/user/authentication
Similarity	There are some users whose biometric information is nearly identical to others

Embedded Systems, Table 2 Vulnerabilities common to general IT systems

Name of vulnerability	Definitions
Registration	Vulnerability upon registration
Singularity	Available to attack against anyone else's IDs without any tools when biometric information is simply used
Alternative Means	There always need certain means alternable for biometric authentication as there are some people who cannot be authenticated by or there are those whose biometric data cannot be obtainable from
Presence	Biometric information is presentable to third party/people if the owner grants
Motivation	Verifiable/identifiable data entry is necessary by the user of biometric system
Sensor Exposure	Sensor which collecting biometric data is disclosed to outside
Data Leakage	Leakage of biometric data stored in biometric system to outside
Side-channel	Leakage of the information relevant to biometric system to outside
Data Alteration	Alteration availability for those data stored in biometric system
Configuration Management	Upon differed conformity in elements which configuring system, normal operation and matching performance required are getting disabled
Deactivation	Authentication is getting unavailable temporarily when some parameters are satisfied

those biometric specific and those common to general information systems. However, in the latter case, only those that may cause a threat when combined with the biometric-specific vulnerability(ies) are listed. Table 3 shows the vulnerabilities in biometric systems in the respective phases: Planning, Development, Operational, and Discard.

Related Entries

▸ Biometrics, Overview

Embedded Systems, Table 3 Lifecycle of embedded systems and their vulnerabilities

	Name of vulnerability	Planning	Development	Operational	Discard
Biometric System-Specific Vulnerabilities	Familiarity/Proficiency			Y	
	Acceptability			Y	
	FAR (False Acceptance Rate)			Y	
	FRR (False Resistance Rate)			Y	
	Unavailability			Y	
	User Status			Y	
	Entering Environment (Minutia Angle, etc.)			Y	
	Wolf			Y	
	Lamb			Y	
	Goat			Y	
	Authentication Parameter			Y	
	Falsified Biometric Information			Y	
	Publication			Y	
	Assumption			Y	Y
	Extent	Y	Y		
	Similarity			Y	
Vulnerabilities common to general IT systems	Registration			Y	
	Singularity			Y	
	Alternative Means			Y	
	Presence			Y	Y
	Motivation			Y	
	Sensor Exposure		Y	Y	
	Data Leakage			Y	Y
	Side-channel			Y	Y
	Data Alteration		Y	Y	
	Configuration Management		Y	Y	
	Deactivation			Y	

References

1. T.A. Henzinger, J. Sifakis, The discipline of embedded systems design, IEEE Comput. **40**, 32–40 (2007)
2. D.D. Hwang, P. Schaumont, K. Tiri, I. Verbauwhede, Securing embedded systems. IEEE Secur. Priv. **4**, 40–49 (2006)
3. A.K. Jain, R. Bolle, S. Pankanti, *Biometrics: Personal Identification in Networked Society* (Kluwer Academic, Norwell, 1998)
4. A.K. Jain, A. Ross, S. Pankanti, An introduction to biometric recognition. IEEE T. Circuits. Syst. Video. Technol. **14**(1), 4–20 (2004)
5. M. Faundez-Zanuy, On the vulnerability of biometric security systems. IEEE Aerosp. Electron. Syst. Mag. **19**(6), 3–8 (2004)

Encryption, Biometric

Ann Cavoukian and Alex Stoianov
Office of the Information and Privacy Commissioner, Toronto, ON, Canada

Synonyms

Biometric cryptosystem; Biometric key generation; Biometric locking; Fuzzy extractor; Secure sketch

Definition

Biometric Encryption (BE) is a group of emerging technologies that securely bind a digital key to a biometric or generate a digital key from the biometric, so that no biometric image or template is stored. What is stored is the BE template otherwise known as a "biometrically encrypted key" or "helper data." As a result, neither the digital key nor the biometric can be retrieved from the stored BE template. BE conceptually differs from other systems that encrypt biometric images or templates using conventional encryption or store a cryptographic key and release it upon successful biometric authentication. With BE, the digital key is recreated only if the correct biometric sample is presented on verification. The output of BE verification is either a digital key or a failure message. This "encryption/decryption" process is fuzzy because of the natural variability of biometric samples. Currently, any viable BE system requires that biometric-dependent helper data be stored.

Introduction

Biometric technologies may add a new level of authentication and identification to applications but are not, however, without their risks and challenges. There are important technological challenges such as accuracy, reliability, data security, user acceptance, cost, and interoperability, as well as challenges associated with ensuring effective privacy protections. Some common security vulnerabilities of biometric systems include:

Spoofing, replay attacks, substitution attacks, tampering, masquerade attacks (creating a digital "artifact" image from a fingerprint template so that this artifact, if submitted to the system, will produce a match), Trojan horse attacks, and overriding yes/no response (which is an inherent flaw of existing biometric systems).

In addition to the security threats that undermine the reliability of biometric systems, there are a number of specific privacy concerns with these technologies:

- Function creep (i.e., unauthorized secondary uses of biometric data)
- Expanded surveillance, tracking, profiling, and potential discrimination (biometric data can be matched against samples collected and stored elsewhere and used to make decisions about individuals)
- Data misuse (data breach, identity theft, and fraud)
- Negative personal impacts of false matches, non-matches, system errors, and failures (the consequences of system anomalies, especially in large-scale systems, often fall disproportionately on individuals, normally in the form of inconveniences, costs, and stigma)
- Insufficient oversight, accountability, and openness in biometric data systems
- Potential for collection and use of biometric data without knowledge, consent, or personal control

These types of risks threaten user confidence, which leads to a lack of acceptance and trust in biometric systems.

Biometric Encryption (BE) technologies can help to overcome the prevailing "zero-sum" mentality involved in traditional biometrics, namely, that adding privacy to authentication and information systems weakens security. With BE, it is possible to enhance both privacy and security in a positive-sum model.

What Is Biometric Encryption (BE)?

The concept of Biometric Encryption (BE) was first introduced in the mid-1990s by G. Tomko et al. [1]. For more information on BE and related technologies, see the review papers in [2–4].

Biometric Encryption is a process that securely binds a digital key to a biometric or generates a key from the biometric. In essence, the key is "encrypted" with the biometric, and the resulting biometrically encrypted key, also called BE template or helper data, is stored. The digital key can be "decrypted" on verification if a correct biometric sample is presented. This "encryption/decryption" process is fuzzy by nature, because the biometric sample is different each

time, unlike an encryption key in conventional cryptography. A major technological challenge is to have the same digital key recreated despite the natural variations in the input biometrics.

After the digital key is recreated on verification, it can be used as the basis for any physical or logical application. The most obvious use is in a conventional cryptosystem where the key serves as a password and may generate, for example, a pair of Public and Private keys. It should be noted that BE itself is not a cryptographic algorithm. The role of BE is to replace or augment vulnerable password-based schemes with more secure and more convenient biometrically managed keys.

BE should not be mistaken for other systems that encrypt biometric images or templates using conventional encryption or store a cryptographic key in a trusted token/device and subsequently release it upon successful biometric verification (i.e., after receiving yes response). However, BE is related to another family of privacy-enhancing technologies called Cancelable Biometrics (CB) (N. Ratha et al. in [3]; see also the Encyclopedia article on "▶ Cancelable Biometrics"). CB applies a transform (preferably, non-invertible) to a biometric image or template and matches the CB templates in the transformed domain. This transform is usually kept secret. Unlike BE, the CB system does not bind or generate a key. CB remains inherently vulnerable to overriding yes/no response and to a substitution attack.

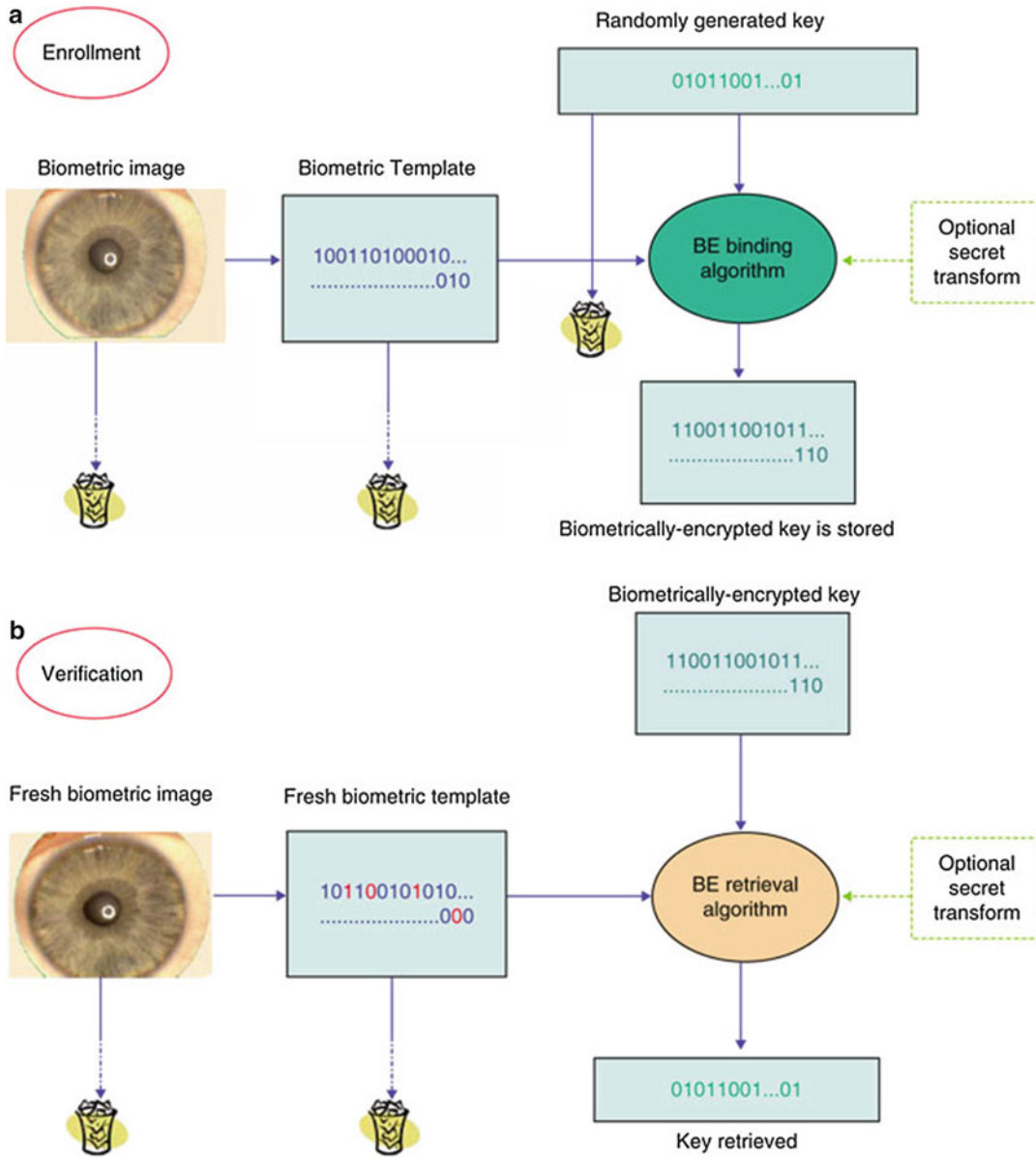
There are two BE approaches: key binding, when an arbitrary key (e.g., randomly generated) is securely bound to the biometric, and key generation, when a key is derived from the biometric. Both approaches usually store biometric-dependent helper data. Some BE schemes (e.g., Fuzzy Commitment [5], Fuzzy Vault [6]) can equally work in both key generation and key binding mode; the key generation is also called "secure sketch" or "fuzzy extractor" as defined in [7]. Secure sketch implies that the enrolled biometric template will be recovered on verification when a fresh biometric sample is applied to the helper data (i.e., the enrolled template itself or a string derived from it, e.g., by hashing the template, serves as a digital key). Note, however, that this "key" is not something inherent or absolute for this particular biometric; it will change upon each re-enrollment. The size of the key space for the secure sketch is defined by the intraclass variations of the biometric as opposed to the key binding approach.

In the key binding mode, as illustrated in Fig. 1, the digital key is randomly generated on enrollment so that neither the user nor anybody else knows it. The key itself is completely independent of biometrics and, therefore, can always be changed or updated. After a biometric sample is acquired, the BE algorithm securely and consistently binds the key to the biometric to create a biometrically encrypted key. The BE template provides privacy protection and can be stored either in a database or locally (smart card, token, laptop, cell phone, etc.). At the end of the enrollment, both the key and the biometric are discarded.

On verification, the user presents his or her fresh biometric sample, which, when applied to the legitimate BE template, will let the BE algorithm recreate the same key. At the end of verification, the biometric sample is discarded once again. The BE algorithm is designed to account for acceptable variations in the input biometric. On the other hand, an impostor whose biometric sample is different enough will not be able to recreate the key.

Many BE schemes also store a hashed value of the key (not shown in Fig. 1) so that a correct key is released from the BE system only if the hashed value obtained on verification is exactly the same. Also, good practice would be not to release the key but, rather, another hashed version of it for any application. This hashed version can in turn serve as a cryptographic key. With this architecture, an attacker would not be able to obtain the original key outside the BE system. Likewise, the biometric image/template should not be sent to a server; the BE verification should be done locally in most scenarios.

An important part of most BE algorithms is an error-correcting code (ECC). ECCs are used in communications, for data storage, and in other systems where errors can occur. Biometric Encryption is a new area for the application of



Encryption, Biometric, Fig. 1 High-level diagram of a Biometric Encryption process in a key binding mode. **(a)** Enrollment; **(b)** Verification

ECC. For example, a binary block ECC, which is denoted (n, k, d), encodes k bits with $n > k$ bits by adding some redundancy. Those n-bit strings are called codewords; there are 2^k of them in total, where k is the key length. The minimum distance (usually a Hamming distance is implied) between the codewords is d. If, at a later stage (in case of BE, on verification), the errors occur, the ECC is guaranteed to correct up to $(d-1)/2$ bit errors among n bits. Ideally, the legitimate users will have a number of errors within the ECC bound so that the ECC will decode the original codeword and, hence, the digital key. On the other hand, the impostors will produce an uncorrectable number of errors, in which case the ECC (and the BE algorithm as a whole) will declare a failure.

In practice, BE, like any biometric system, has both false rejection and false acceptance rates (FRR and FAR). Note that BE does not use any matching score; instead, the FRR/FAR tradeoff may be achieved in some cases by varying the parameters of the BE scheme. Some ECCs may work in a soft decoding mode, that is, the decoder always outputs the nearest codeword, even if it is beyond the ECC bound. This allows achieving better error-correcting capabilities.

To improve the security of a BE system, an optional "transform in the middle" (shown in the dashed square in Fig. 1) may be applied. Preferably, the transform should be non-invertible and kept secret. One of the ways would be employing a randomization technique, such as Biohashing [8] or "salting" in more general terms [2]. The transform can be controlled with the user's password or can be separated from the rest of the helper data by storing it on a token or a server.

Advantages and Possible Applications of BE

BE technologies can enhance both privacy and security in the following ways:

- There is no retention of biometric image or conventional biometric template, and they cannot be recreated from the stored helper data.
- They are capable of multiple identifiers: A large number of BE templates for the same biometric can be created for different applications.
- The BE templates from different applications cannot be linked.
- The BE template can be revoked or canceled.
- They can be easily integrated into conventional cryptosystems, as the passwords are replaced with longer digital keys, which do not have to be memorized.
- They provide improved authentication and personal data security through a stronger binding of user biometric and system identifier.
- The BE systems are inherently protected from substitution attack, tampering, Trojan horse attack, and overriding yes/no response and less susceptible to masquerade attack.
- They are suitable for large-scale applications, as the databases will store only untraceable, yet sufficient, information to verify the individual's claim.

These features embody standard fair information principles, providing user control, data minimization, and data security.

As such, BE technologies put biometric data firmly under the exclusive control of the individual, in a way that benefits the individual and minimizes the risk of function creep and identity theft. They provide a foundation for building greater public confidence, acceptance, and use and enable greater compliance with privacy and data protection laws.

Possible applications and uses of Biometric Encryption include:

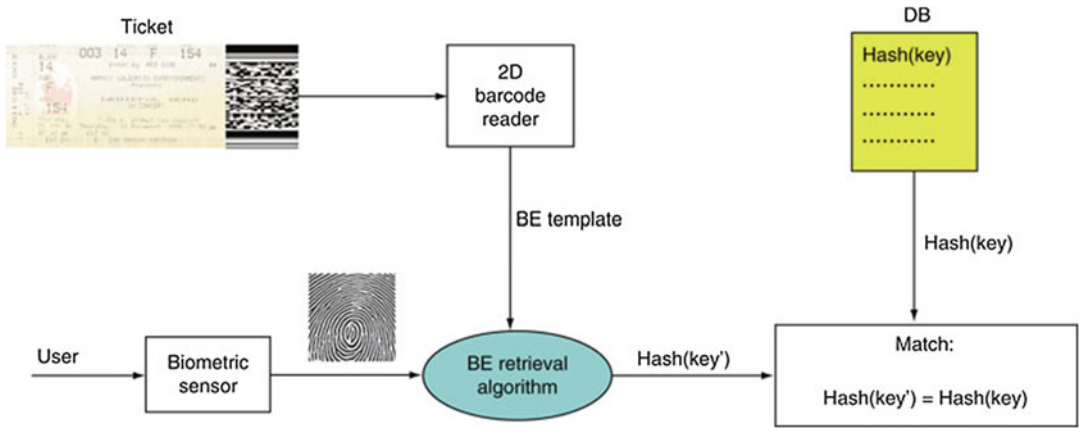
- Biometric ticketing (Fig. 2) for events
- Biometric boarding cards for travel
- Drug prescriptions
- Three-way check of travel documents
- Identification, credit, and loyalty card systems
- Anonymous databases (Fig. 3), that is, anonymous (untraceable) labeling of sensitive records (medical, financial)
- Consumer biometric payment systems
- Remote authentication via challenge-response scheme
- Access control (physical and logical)
- Personal encryption products (i.e., encrypting files, drives, e-mails, etc.)
- Local or remote authentication of users to access files held by government and other various organizations

BE Technologies

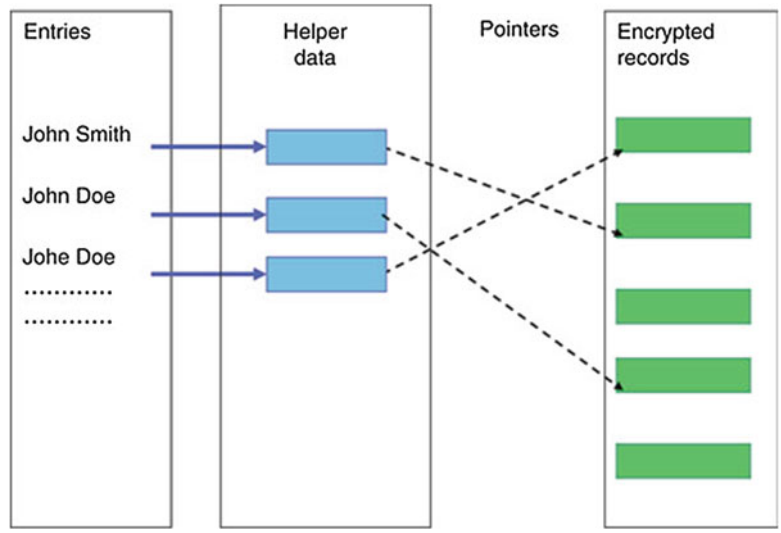
The following are core BE schemes. The more detailed, up-to-date overviews of BE technologies are presented in [2, 4].

Mytec1

This is the first BE scheme [1]. It was developed using optical processing but can also be implemented digitally. The key is linked to a



Encryption, Biometric, Fig. 2 Biometric ticketing. A BE template is stored on a ticket as a 2D bar code, and a database stores the hashed value of a key, Hash(key), for each enrolled user. The key and the ticket are used only for this particular application. On a verification terminal: (i) The user presents his ticket to the system which reads in the BE template from the bar code; (ii) the live biometric sample is taken; (iii) the system applies the biometric to the BE template to retrieve the key; (iv) Hash(key') is sent to the database where it is compared to the stored version, Hash(key)



Encryption, Biometric, Fig. 3 Anonymous database controlled by Biometric Encryption. The database contains anonymous encrypted records, e.g., medical files. The cryptographic keys and the links to the entries, which may be users' names or pseudonyms, are controlled by BE. After the user enters his pseudonym, the associated BE template (helper data) is retrieved and applied to the user's biometric. If BE successfully recovers the user's digital key, it will recreate the pointer to the anonymous record and the encryption key to decrypt the record

predefined pattern, s(x), which is a sum of several delta functions. Using s(x) and a fingerprint, f(x), one can create a filter, $H(u) = S(u)/F(u)$, in Fourier domain (S(u) and F(u) are the Fourier transforms of s(x) and f(x)). It is difficult to obtain either S(u) or F(u) from the stored filter H(u). On verification, if a correct fingerprint, $F'(u) \approx F(u)$, is applied to the filter, it will reconstruct a correct output pattern, $s'(x) \approx s(x)$, so that the key will be regenerated from the locations of

the output correlation peaks. Unfortunately, this scheme turned out to be impractical in terms of providing sufficient accuracy and security.

Mytec2

This is the first practical BE scheme [9]. Unlike Mytec1, it retains phase-only parts of S(u) and F(u) in the filter, H(u). The phase of S(u) is randomly generated but not stored anywhere. As a result, the output pattern, c(x), is also random. The key, normally 128-bit long, is linked to c(x) via a lookup table and ECC. The filter, H(u), the lookup table, and the hashed key are stored in the helper data. The system is error tolerant and translation invariant. The published version [9] used a simple repetition ECC, which makes the system vulnerable to several attacks, such as hill climbing [10].

However, a closer examination of the Mytec2 scheme shows that if the randomness of H(u) and c(x) is preserved on each step of the algorithm, the scheme is a variant of so-called permutation-based fuzzy extractor as defined in [7]. Therefore, if a proper ECC (preferably, single block) is used instead of the repetition ECC, the system will be as secure as those types of fuzzy extractors.

(Note that Mytec1 and Mytec2 schemes were originally called "Biometric Encryption," which was a trademark of Toronto-based Mytec Technologies Inc., now Bioscrypt, a fully owned subsidiary of L1 Identity Solutions Inc. The trademark was abandoned in 2005.)

ECC Check Bits

This scheme, which was originally called "private template," is a secure sketch (i.e., a key generation) [11]. A biometric template itself serves as a cryptographic key. To account for the template variations between different biometric samples, an (n, k, d) error- correcting code is used. A number of (n-k) bits, called *check bits*, are appended to the template to map the k-bit template to an n-bit codeword. The check bits are stored into the helper data along with the hashed value of the template. The scheme is impractical, since it is required that $n < 2k$ from the security perspective. Such ECC would not be powerful enough to correct a realistic number of errors for most biometrics, including iris scan.

Biometrically Hardened Passwords

This technique was developed for keystroke dynamics or voice recognition [12]. A password that the user types or says is fused with a key (via a secret sharing scheme) extracted from a biometric component, thus hardening the password with the biometrics. The technique was made adaptive by updating a "history file" (which is, in fact, helper data) upon each successful authentication. However, the types of biometrics used did not allow for achieving good accuracy numbers.

Fuzzy Commitment

This is conceptually the simplest, yet the most studied, BE scheme [5] (A. Juels in [3]). A biometric template must be in the form of an ordered bit string of a fixed length. A key is mapped to an (n, k, d) ECC codeword of the same length, n, as the biometric template. The codeword and the template are XOR-ed, and the resulting n-bit string is stored into helper data along with the hashed value of the key. On verification, a fresh biometric template is XOR-ed with the stored string, and the result is decoded by the ECC. If the codeword obtained coincides with the enrolled one (this is checked by comparing the hashed values), the k-bit key is released. If not, a failure is declared.

In a "secure sketch" (i.e., key generation) mode [7], the enrolled template is recovered from the helper data on verification, if a correct (yet different) biometric sample is presented.

The scheme seems to be one of the best for the biometrics where the proper alignment of images is possible, such as iris scan [13, 14] and face recognition (T. Kevenaar in [3]). For iris, the reported results are FRR = 0.47 % at FAR $< 10^{-5}$ for a 140-bit key mapped to 2,048-bit codeword [13] and FRR = 5.6 % at FAR $< 10^{-5}$ (42-bit key) [14] for a poorer quality, yet more realistic, iris database.

ECC Syndrome

In this spinoff of the Fuzzy Commitment scheme, a so-called ECC syndrome of (n-k) size is stored in the helper data [2, 7]. On verification, the enrolled template is recovered (i.e., the scheme works in the secure sketch mode).

Quantization Using Correction Vector

This method, which was also called "shielding functions," is applied to continuously distributed and aligned biometric features (J.-P. Linnartz et al. in [3]). For each feature, a residual is calculated, which is the distance to the center of the nearest even-odd or odd-even interval, depending on the parity of the key bit. The correction vector comprising all the residuals is stored into the helper data. On verification, a noisy feature is added to the residual and is decoded as 1 or 0, if the resulting interval is odd-even or vice versa. The scheme can work with or without (if a noise level is low) a subsequent ECC. In general, storing a correction vector could make the scheme vulnerable to score-based attacks.

Fuzzy Vault

This is, probably, the only BE scheme that is fully suitable for unordered data with arbitrary dimensionality, such as fingerprint minutiae [6, 15]. A secret message (i.e., a key) is represented as coefficients of a polynomial in a Galois field, for example, GF(2^{16}). In the most advanced version [15], the 16-bit x-coordinate value of the polynomial comprises the minutia locations and the angle, and the corresponding y-coordinates are computed as the values of the polynomial on each x. Both x and y numbers are stored alongside with chaff points that are added to hide real minutiae. On verification, a number of minutiae may coincide with some of the genuine stored points. If this number is sufficient, the full polynomial can be reconstructed using an ECC (e.g., Reed-Solomon ECC) or Lagrange interpolation. The polynomial reconstruction means that the secret has been successfully decrypted. The scheme works both in the key binding and the key generation (secure sketch) mode. The version of [15] also stores fingerprint alignment information. The best results for fingerprints show FRR = 6–17 % at FAR = 0.02 %.

The more secure version of Fuzzy Vault [7] stores high-degree polynomial instead of real minutiae or chaff points. However, there are difficulties in the practical implementation of this version.

Unlike other BE schemes, the Fuzzy Vault actually stores real minutiae, even though they are buried inside the chaff points. This could become a source of potential vulnerabilities [2,4]. The system security can be improved by applying a secret minutiae permutation controlled by a user's password [2]. This "transform-in-the-middle" approach is applicable to most BE schemes.

Biohashing (with Key Binding)

An ordered biometric feature set is transformed into a new space of a lower dimension by generating a random set of orthogonal vectors and obtaining an inner product between each vector and the biometric feature set [8]. The result (called "Biohash") is binarized to produce a bit string. The random feature vectors are generated from a random seed that is kept secret, for example, by storing it in a token. The key is bound to the Biohash via Shamir secret sharing with linear interpolation or by using a standard Fuzzy Commitment scheme. Very good FRR/FAR numbers [8] were obtained, however, in an unrealistic "non-stolen token" scenario. Biohashing is referred more often as a CB scheme where Biohashes are matched directly, that is, without the key binding.

Graph-Based Coding

In this generalization of the ECC syndrome scheme, Low-Density Parity Check (LDPC) ECCs are used in a graphical representation [16]. LDPC codes, which are the state-of-the-art channel ECCs (n, k, d), can be designed with large numbers of n and k and can handle high error rates. This makes them suitable for BE applications. The scheme can be applied to both ordered (e.g., iris) and unordered (e.g., fingerprint minutiae) feature

sets. For the latter, a factor graph models the minutiae variability as a movement, an erasure, or an insertion (i.e., spurious generation) of minutiae. The scheme uses a belief propagation decoding algorithm and shows promising results.

Attacks on BE

Despite the fact that many BE schemes have a formal proof of security, they may be vulnerable to low level attacks, such as when an attacker has access to helper data, is familiar with the BE algorithm, and can run the attack offline. By cracking a BE system, the attacker can pursue one or more of the following:

- Obtain the key bound to the biometrics
- Obtain the exact biometric template used on enrollment
- Obtain an approximate version of the template that, nonetheless, would defeat the system (masquerade template)
- Create a masquerade image of the biometrics
- Link BE templates generated from the same biometrics but stored in different databases

The known attacks on BE, as described in [4], are listed in the following paragraphs. Note that CB may also be vulnerable to most of the attacks.

False acceptance attack. This is one of the "brute force" attacks. Offline, the attacker runs an impostor database of about FAR^{-1} biometric images or templates against the helper data to obtain a false acceptance. The database can be either real or computer generated, such as *SFinGe*. The image that has generated the false acceptance will serve as a masquerade image.

Reversing the hash. This is another "brute force" attack. If a hashed key is stored into the helper data, the attacker may try to cryptographically reverse the hash. This attack should always be made more computationally expensive for an attacker than other attacks.

Hill climbing attack [10]. Based on the knowledge of the algorithm, the attacker derives an intermediate matching score during the verification process, even though the BE algorithm does not use any score. By making small changes in the input impostor's image or template, the attacker retains the change, if the score increases, or rejects it, if not. After a number of iterations, the attacker may be able to retrieve a key and create a masquerade image/template.

The BE schemes that divide helper data into short chunks of ECC (e.g., a repetition ECC) and the schemes with a correction vector may be especially vulnerable to this and to the nearest impostor's attack.

Nearest impostor's attack [4]. This is another score-based attack. The attacker derives a partial matching score for each ECC chunk (if any) of the helper data and a global intermediate score (like in the hill climbing attack). By running a small impostor database against the helper data, the attacker identifies several "nearest impostors," that is, the attempts with the highest global score or, alternatively, with the highest partial score for a given chunk. By applying a voting technique to the nearest impostors, the attacker retrieves the key bits associated with the chunk. If successful, the attack yields the entire key or at least reduces the search space for the key.

Using statistics of ECC output [4]. A small impostor database (with various distortions, rotations, and shifts applied) is run against the ECC chunks of the helper data. The number of appearances of each possible output codeword for all impostor attempts is counted to create a histogram. The codeword corresponding to the histogram maximum is declared a winner.

Using an information leak from helper data. This group of attacks may directly exploit:

- Nonrandomness of the helper data [4] (e.g., if clusters in the helper data are identified, the attacker may interconnect the same parity bits)
- Alignment information and minutiae angles in the Fuzzy Vault
- A method for generating the chaff points [17]
- Nonuniformity of the output bits distribution in quantization schemes, etc.

Reusability attack (X. Boyen in [3]). If the same biometric is reused for different applications and/or keys, the attacker may combine several versions of the helper data to retrieve both the biometric and all the keys. Fuzzy Vault is especially vulnerable to this attack.

Among all BE schemes, it seems that one of the most secure would be a Fuzzy Commitment (or other related fuzzy extractors, such as ECC syndrome) scheme with a single block (n, k, d) ECC, where n and k are large (e.g., $n > \sim 1{,}000$, $k > \sim 100$). From the security perspective, the amount of any additional side information that is stored (e.g., alignment data) should be kept to a minimum.

The resilience to some of the attacks may be improved by employing the "transform-in-the-middle" approach, especially if the transform is controlled by a password/token.

Current State of BE

Many different approaches have been developed for BE, but currently few systems have been deployed or implemented into products. Until now, little work has been done to analyze the security of BE systems.

The authors consider the following technologies as the state of the art of BE:

- Philips (the Netherlands) priv-ID™ for the face recognition (2D and 3D) and fingerprints (T. Kevenaar in [3])
- Hao et al. for iris [13]
- Nandakumar et al. (Fuzzy Vault for fingerprints) [15]
- Draper et al. of Mitsubishi Electric Research Laboratories (USA) for iris and fingerprints [16]
- Bringer et al. of Sagem Sécurité (France) for iris [14]
- Genkey (Norway) BioCryptic® for fingerprints (unfortunately, not much information about the technology is available)

The Philips priv-ID™ technology is ready for deployment. It is part of the EU 3D Face project and of the 3-year EU TURBINE project [18]. The latter has been given significant funding and aims at piloting a fingerprint-based BE technology at an airport in Greece.

The Genkey BioCryptic® technology has been deployed for a Rickshaw project in New Delhi (India). Both Philips and Genkey systems can fit the helper data into a 2D bar code.

BE Challenges

Technologically, BE is much more challenging than conventional biometrics, since most BE schemes work in a "blind" mode (the enrolled image or template are not seen on verification). As BE advances to the next phase of creating and testing a prototype, the following issues need to be addressed:

- Biometric modalities that satisfy the requirements of high entropy, low variability, possibility of alignment, and public acceptance should be chosen. At present, the most promising biometric for BE is iris followed by fingerprints and face.
- The image acquisition process (the requirements are tougher for BE than for conventional biometrics) must be improved.
- BE must be made resilient against attacks.
- The overall accuracy and security of BE algorithms must be improved. Advances in the algorithm development in conventional biometrics and in ECCs should be applied to BE.
- Multimodal approaches should be exploited.
- BE applications should be developed.

Summary

Biometric Encryption is a fruitful area for research and is becoming sufficiently mature for prototype development and the consideration of applications.

BE technologies exemplify the fundamental privacy and data protection principles that are endorsed around the world, such as data minimization, user empowerment, and security.

Although introducing biometrics into information systems may result in considerable benefits, it can also introduce many new security and privacy vulnerabilities, risks, and concerns. Novel Biometric Encryption techniques can overcome many of those risks and vulnerabilities, resulting in a win-win, positive-sum model that presents distinct advantages to both security and privacy.

Related Entries

- Biometric Vulnerabilities, Overview
- Cancelable Biometrics
- Security and Liveness, Overview
- SFinGe
- Template Security

References

1. G.J. Tomko, C. Soutar, G.J. Schmidt, Fingerprint controlled public key cryptographic system. U.S. Patent 5,541,994, 30 July 1996 (Filing date: 7 Sept 1994)
2. A.K. Jain, K. Nandakumar, A. Nagar, Biometric template security. EURASIP J. Adv. Signal Process. **2008**, 1–17 (2008). Article ID 579416
3. P. Tuyls, B. Škorić, T. Kevenaar (eds.), *Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting* (Springer, London, 2007)
4. A. Cavoukian, A. Stoianov, Biometric encryption: the new breed of untraceable biometrics, in *Biometrics: Fundamentals, Theory, and Systems*, ed. by N.V. Boulgouris, K.N. Plataniotis, E. Micheli-Tzanakou (Wiley, London, 2009)
5. A. Juels, M. Wattenberg, A fuzzy commitment scheme, in *Sixth ACM Conference on Computer and Communications Security*, Singapore, ed. by G. Tsudik (ACM, New York, 1999), pp. 28–36
6. A. Juels, M. Sudan, A fuzzy vault scheme, in *Proceedings of IEEE International Symposium on Information Theory*, Palais de Beaulieu, Lausanne, ed. by A. Lapidoth, E. Teletar (IEEE, Lausanne, 2002), p. 408
7. Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, in ed. by C. Cachin, J. Camenish, *Proceedings if Eurocrypt 2004* (Springer, New York, 2004), pp. 523–540
8. A.B.J. Teoh, D.C.L. Ngo, A. Goh, Personalised cryptographic key generation based on FaceHashing. Comput. Secur. **23**, 606–614 (2004)
9. C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B.V.K. Vijaya Kumar, Biometric encryption (Chapter 22), in *ICSA Guide to Cryptography*, ed. by R.K. Nichols (McGraw-Hill, New York, 1999)
10. A. Adler, Vulnerabilities in biometric encryption systems, in *Audio- and Video-Based Biometric Person Authentication (AVBPA2005)*. Lecture Notes in Computer Science, vol. 3546 (Springer, New York, 2005), pp. 1100–1109
11. G.I. Davida, Y. Frankel, B.J. Matt, On enabling secure applications through off-line biometric identification, in *Proceedings of the IEEE 1998 Symposium on Security and Privacy*, Oakland (1998), pp. 148–157
12. F. Monrose, M.K. Reiter, S. Wetzel, Password hardening based on keystroke dynamics. Int. J. Inf. Secur. **1**(2), 69–83 (2002)
13. F. Hao, R. Anderson, J. Daugman, Combining crypto with biometrics effectively. IEEE Trans. Comput. **55**(9), 1081–1088 (2006)
14. J. Bringer, H. Chabanne, G. Cohen, Kindarji, G. Z'emor, Optimal iris fuzzy sketches, in *IEEE First International Conference on Biometrics: Theory, Applications, and Systems, BTAS'07*, Washington, D.C., 27–29 Sept 2007
15. K. Nandakumar, A.K. Jain, S.C. Pankanti, Fingerprint-based fuzzy vault: implementation and performance. IEEE Trans. Inf. Forensics Secur. **2**(4), 744–757 (2007)
16. S.C. Draper, A. Khisti, E. Martinian, A. Vetro, J.S. Yedidia, Using distributed source coding to secure fingerprint biometrics, in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Honolulu, vol. 2 (2007), pp. 129–132
17. E.-C. Chang, R. Shen, F.W. Teo, Finding the original point set hidden among chaff, in *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security (ASIACCS'06)*, Taipei, Sept 2006, pp. 182–188
18. N. Delvaux, J. Bringer, J. Grave, K. Kratsev, P. Lindeberg, J. Midgren, J. Breebaart, T. Akkermans, M. van der Veen, R. Veldhuis, E. Kindt, K. Simoens, C. Busch, P. Bours, D. Gafurov, B. Yang, J. Stern, C. Rust, B. Cucinelli, D. Skepastianos, Pseudo identities based on fingerprint characteristics, in *IEEE Fourth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2008)*, Harbin, 15–17 Aug 2008

Ensemble Learning

Zhi-Hua Zhou
National Key Lab for Novel Software Technology, Nanjing University, Nanjing, China

Synonyms

Classifier combination; Committee-based learning; Multiple classifier systems

Definition

Ensemble learning is a machine learning paradigm where multiple learners are trained to solve the same problem. In contrast to ordinary machine learning approaches which try to learn

one hypothesis from training data, ensemble methods try to construct a *set* of hypotheses and combine them to use.

Introduction

An ensemble contains a number of learners which are usually called *base learners*. The generalization ability of an ensemble is usually much stronger than that of base learners. Actually, ensemble learning is appealing because it is able to boost *weak learners* which are slightly better than random guess to *strong learners* which can make very accurate predictions. So, "base learners" are also referred to as "weak learners." It is noteworthy, however, that although most theoretical analyses work on weak learners, base learners used in practice are not necessarily weak since using not-so-weak base learners often results in better performance.

Base learners are usually generated from training data by a *base learning algorithm* which can be decision tree, neural network, or other kinds of machine learning algorithms. Most ensemble methods use a single base learning algorithm to produce *homogeneous* base learners, but there are also some methods which use multiple learning algorithms to produce *heterogeneous* learners. In the latter case there is no single base learning algorithm, and thus, some people prefer calling the learners *individual learners* or *component learners* to "base learners," while the names "individual learners" and "component learners" can also be used for homogeneous base learners.

It is difficult to trace the starting point of the history of ensemble methods since the basic idea of deploying multiple models has been in use for a long time, yet it is clear that the hot wave of research on ensemble learning since the 1990s owes much to two works. The first is an applied research conducted by Hansen and Salamon [1] at the end of 1980s, where they found that predictions made by the combination of a set of classifiers are often more accurate than predictions made by the best single classifier. The second is a theoretical research conducted in 1989, where Schapire [2] proved that *weak learners* can be boosted to *strong learners*, and the proof resulted in boosting, one of the most influential ensemble methods.

Constructing Ensembles

Typically, an ensemble is constructed in two steps. First, a number of base learners are produced, which can be generated in a *parallel* style or in a *sequential* style where the generation of a base learner has influence on the generation of subsequent learners. Then, the base learners are combined to use, where among the most popular combination schemes are majority voting for classification and *weighted averaging* for regression.

Generally, to get a good ensemble, the base learners should be as more accurate as possible and as more diverse as possible. This has been formally shown by Krogh and Vedelsby [3] and emphasized by many other people. There are many effective processes for estimating the *accuracy* of learners, such as cross-validation, hold-out test, etc. However, there is no rigorous definition on what is intuitively perceived as *diversity*. Although a number of diversity measures have been designed, Kuncheva and Whitaker [4] disclosed that the usefulness of existing diversity measures in constructing ensembles is suspectable. In practice, the diversity of the base learners can be introduced from different channels, such as subsampling the training examples, manipulating the attributes, manipulating the outputs, injecting randomness into learning algorithms, or even using multiple mechanisms simultaneously. The employment of different base learner generation processes and/or different combination schemes leads to different ensemble methods.

There are many effective ensemble methods. The following will briefly introduce three representative methods: *boosting* [2, 5], *bagging* [6] and *stacking* [7]. Here, binary classification is considered for simplicity. That is, let $\mathcal{X}$

Input: Data set $\mathcal{D} = \{(x_1, y_1), (x_2, y_2), \cdots, (x_m, y_m)\}$;
Base learning algorithm $\mathcal{L}$;
Number of learning rounds T.

Process:
$D_1(i) = 1/m$. % initialize the weight distribution
for $t = 1, \cdots, T$:
$h_t = \mathcal{L}(\mathcal{D}, D_t)$; % Train a base learner h_t from $\mathcal{D}$ using distribution D_t
$\epsilon_t = \Pr_{i \sim D_i}[h_t(x_i) \neq y_i)]$; % Measure the error of h_t
$\alpha_t = \frac{1}{2} \ln\left(\frac{1-\epsilon_t}{\epsilon_t}\right)$; % Determine the weight of h_t

$$D_{t+1}(i) = \frac{D_t(i)}{Z_t} \times \begin{cases} \exp(-\alpha_t) & \text{if } h_t(x_i) = y_i \\ \exp(\alpha_t) & \text{if } h_t(x_i) \neq y_i \end{cases}$$

$$= \frac{D_t(i)\exp(-\alpha, y, h, (x_i))}{Z_t}$$

% Update the distribution, where Z_t is a normalization % factor which enables D_{t+1} to be a distribution

end.

Output: $H(x) = \text{sign}(f(x)) = \text{sign}(\Sigma_{t=1}^{T} \alpha_t h_t(x))$

Ensemble Learning, Fig. 1 The AdaBoost algorithm

and $\mathcal{Y}$ denote the instance space and the set of class labels, respectively, assuming $\mathcal{Y} = \{-1, +1\}$. A training data set $\mathcal{D} = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \cdots, (\mathbf{x}_m, y_m)\}$ is given, where $\mathbf{x}_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$ $(i = 1, \ldots, m)$.

Boosting is in fact a family of algorithms since there are many variants. Here, the most famous algorithm, AdaBoost [5], is considered as an example. First, it assigns equal weights to all the training examples. Denote the distribution of the weights at the t-th learning round as D_t. From the training data set and D_t, the algorithm generates a base learner $h_t : \mathcal{X} \to \mathcal{Y}$ by calling the base learning algorithm. Then, it uses the training examples to test h_t, and the weights of the incorrectly classified examples will be increased. Thus, an updated weight distribution D_{t+1} is obtained. From the training data set and D_{t+1}, AdaBoost generates another base learner by calling the base learning algorithm again. Such a process is repeated for T times, each of which is called a *round*, and the final learner is derived by weighted majority voting of the T base learners, where the weights of the learners are determined during the training process. In practice, the base learning algorithm may be a learning algorithm which can use weighted training examples directly; otherwise the weights can be exploited by sampling the training examples according to the weight distribution D_t. The pseudo-code of AdaBoost is shown in Fig. 1.

Bagging [6] trains a number of base learners each from a different *bootstrap sample* by calling a base learning algorithm. A bootstrap sample is obtained by subsampling the training data set with replacement, where the size of a sample is the same as that of the training data set. Thus, for a bootstrap sample, some training examples may appear but some may not, where the probability that an example appears at least once is about 0.632. After obtaining the base learners, bagging combines them by majority voting and the most-voted class is predicted. The pseudo-code of bagging is shown in Fig. 2. It is worth mentioning that a variant of bagging, Random Forests [8], has been deemed as one of the most powerful ensemble methods up to date.

In a typical implementation of stacking [7], a number of first-level individual learners are generated from the training data set by employing different learning algorithms. Those individual learners are then combined by a second-level learner which is called as *meta-learner*. The pseudo-code of stacking is shown in Fig. 3. It is evident that stacking has close relation with information fusion methods.

Input: Data set $\mathcal{D} = \{(x_1, y_1), (x_2, y_2), \cdots, (x_m, y_m)\}$;
Base learning algorithm $\mathcal{L}$;
Number of learning rounds T.

Process:
for $t = 1, \cdots, T$:
$\mathcal{D}_t = Bootstrap(\mathcal{D})$; % Generate a bootstrap sample from $\mathcal{D}$
$h_t = \mathcal{L}(\mathcal{D}_t)$ % Train a base learner h_t from the bootstrap sample
end.

Output: $H(x) = \text{argmax}_{y \in \mathcal{Y}} \sum_{t=1}^{T} 1(y = h_t(x))$ % the value of $1(a)$ is 1 if a is $true$ and 0 otherwise

Ensemble Learning, Fig. 2 The bagging algorithm

Input: Data set $\mathcal{D} = \{(x_1, y_1), (x_2, y_2), \cdots, (x_m, y_m)\}$;
First-level learning algorithms $\mathcal{L}_1, \cdots, \mathcal{L}_T$;
Second-level learning algorithm $\mathcal{L}$.

Process:
for $t = 1, \cdots, T$:
$h_t = \mathcal{L}_t(\mathcal{D})$ % Train a first-level individual learner h_t by applying the first-level
end; % learning algorithm $\mathcal{L}_t$ to the original data set $\mathcal{D}$
$\mathcal{D}' = \emptyset$; % Generate a new data set
for $i = 1, \cdots, m$:
for $t = 1, \cdots, T$:
$z_{it} = h_t(x_i)$ % Use h_t to classify the training example x_i
end;
$\mathcal{D}' = \mathcal{D}' \cup \{((z_{i1}, z_{i2}, \cdots, z_{iT}), y_i)\}$
end;
$h' = \mathcal{L}(\mathcal{D}')$. % Train a second-level learner h' by applying the second-level
% learning algorithm $\mathcal{L}$ to the new data set $\mathcal{D}'$

Output: $H(x) = h'(h_1(x), \cdots, h_T(x))$

Ensemble Learning, Fig. 3 The stacking algorithm

Generally speaking, there is no ensemble method which outperforms other ensemble methods consistently. Empirical studies on popular ensemble methods can be found in many papers such as [9–11]. Previously, it was thought that using more base learners will lead to a better performance, yet Zhou et al. [12] proved the "many could be better than all" theorem which indicates that this may not be the fact. It was shown that after generating a set of base learners, selecting some base learners instead of using all of them to compose an ensemble is a better choice. Such ensembles are called *selective ensembles*.

It is worth mentioning that in addition to classification and regression, ensemble methods have also been designed for clustering [13] and other kinds of machine learning tasks.

Why Ensembles are Superior to Singles

To understand why the generalization ability of an ensemble is usually much stronger than that of a single learner, Dietterich [14] gave three reasons by viewing the nature of machine learning as searching a hypothesis space for the most

accurate hypothesis. The first reason is that the training data might not provide sufficient information for choosing a single best learner. For example, there may be many learners who perform equally well on the training data set. Thus, combining these learners may be a better choice. The second reason is that the search processes of the learning algorithms might be imperfect. For example, even if there exists a unique best hypothesis, it might be difficult to achieve since running the algorithms results in suboptimal hypotheses. Thus, ensembles can compensate for such imperfect search processes. The third reason is that the hypothesis space being searched might not contain the true target function, while ensembles can give some good approximation. For example, it is well known that the classification boundaries of decision trees are linear segments parallel to coordinate axes. If the target classification boundary is a smooth diagonal line, using a single decision tree cannot lead to a good result, yet a good approximation can be achieved by combining a set of decision trees. Note that those are intuitive instead of rigorous theoretical explanations.

There are many theoretical studies on famous ensemble methods such as boosting and bagging, yet it is far from a clear understanding of the underlying mechanism of these methods. For example, empirical observations show that boosting often does *not* suffer from overfitting even after a large number of rounds, and sometimes it is even able to reduce the generalization error after the training error has already reached zero. Although many researchers have studied this phenomenon, theoretical explanations are still in arguing.

The bias-variance decomposition is often used in studying the performance of ensemble methods [9, 12]. It is known that bagging can significantly reduce the variance, and therefore, it is better to be applied to learners who suffered from large variance, e.g., unstable learners such as decision trees or neural networks. Boosting can significantly reduce the bias in addition to reducing the variance, and therefore, on weak learners, such as decision stumps, boosting is usually more effective.

Applications

Ensemble learning has already been used in diverse applications such as optical character recognition, text categorization, face recognition, computer-aided medical diagnosis, gene expression analysis, etc. Actually, ensemble learning can be used wherever machine learning techniques can be used.

Summary

Ensemble learning is a powerful machine learning paradigm which has exhibited apparent advantages in many applications. By using multiple learners, the generalization ability of an ensemble can be much better than that of a single learner. A serious deficiency of current ensemble methods is the lack of comprehensibility, i.e., the knowledge learned by ensembles is not understandable to the user. Improving the comprehensibility of ensembles [15] is an important yet largely understudied direction. Another important issue is that currently no diversity measures are satisfying [4] although it is known that diversity plays an important role in ensembles. If those issues can be addressed well, ensemble learning will be able to contribute more to more applications.

Related Entries

- ▸ Multiple Experts
- ▸ Multiple Classifier Systems
- ▸ Supervised Learning

References

1. L.K. Hansen, P. Salamon, Neural network ensembles. IEEE Trans. Pattern Anal. Mach. Intell. **12**(10), 993–1001 (1990)
2. R.E. Schapire, The strength of weak learnability. Mach. Learn. **5**(2), 197–227 (1990)
3. A. Krogh, J. Vedelsby, Neural network ensembles, cross validation, and active learning, in *Advances in Neural Information Processing Systems*, ed. by G. Tesauro, D.S. Touretzky, T.K. Leen, vol. 7 (MIT, Cambridge, 1995), pp. 231–238

4. L.I. Kuncheva, C.J. Whitaker, Measures of diversity in classifier ensembles and their relationship with the ensemble accuracy. Mach. Learn. **51**(2), 181–207 (2003)
5. Y. Freund, R.E. Schapire, A decision-theoretic generalization of on-line learning and an application to boosting. J. Comput. Syst. Sci. **55**(1), 119–139 (1997)
6. L. Breiman, Bagging predictors. Mach. Learn. **24**(2), 123–140 (1996)
7. D.H. Wolpert, Stacked generalization. Neural Networks **5**(2), 241–260 (1992)
8. L. Breiman, Random forests. Mach. Learn. **45**(1), 5–32 (2001)
9. E. Bauer, R. Kohavi, An empirical comparison of voting classification algorithms: bagging, boosting, and variants. Mach. Learn. **36**(1–2), 105–139 (1999)
10. K.M. Ting, I.H. Witten, Issues in stacked generalization. J. Artif. Intell. Res. **10**, 271–289 (1999)
11. D. Opitz, R. Maclin, Popular ensemble methods: an empirical study. J. Artif. Intell. Res. **11**, 169–198 (1999)
12. Z.H. Zhou, J. Wu, W. Tang, Ensembling neural networks: many could be better than all. Artif. Intell. **137**(1–2), 239–263 (2002)
13. A. Strehl, J. Ghosh, Cluster ensembles – a knowledge reuse framework for combining multiple partitionings. J. Mach. Learn. Res. **3**, 583–617 (2002)
14. T.G. Dietterich, Machine learning research: four current directions. AI Mag. **18**(4), 97–136 (1997)
15. Z.H. Zhou, Y. Jiang, S.F. Chen, Extracting symbolic rules from trained neural network ensembles. AI Commun. **16**(1), 3–15 (2003)

Environmental Testing Methodology of Biometric System Performance, Standardization

Belen Fernandez-Saavedra[1], Judith Liu-Jimenez[2], and Raul Sanchez-Reillo[2]
[1]Science Park, ID Testing Lab, Carlos III University of Madrid, Leganes, Madrid, Spain
[2]GUTI (University Group for Identification Technologies), University Carlos III of Madrid, Leganes, Madrid, Spain

Synonyms

ISO/IEC 29197

Definition

Standard that defines a general and biometric modality-independent evaluation methodology to analyze the influence of environmental conditions on biometric system performance. This methodology is intended for testing biometric performance when biometric systems are working under different environments. This standard has been developed by the international community taking part in ISO/IEC JTC1/SC37 standardization subcommittee [1].

Introduction

Environment is one of the most important aspects that has been traditionally claimed as a factor that influences biometric system performance (see ▸ Influential Factors to Performance). A. Jain, R. Bolle, and S. Pankanti described the dependence of technology performance on the type of application in [2]. They pointed out that the application environment influences directly in the repeatability and distinctiveness of the biometric measure. For this reason they specified seven application categories: cooperative vs. noncooperative, overt vs. covert, habituated vs. non-habituated, attended vs. nonattended, standard environment vs. nonstandard environment, public vs. private, and open vs. closed. In addition, they explained that test results are dependent upon the specific "real-world" application. Lately, this statement was corroborated in other works such as A. J. Mansfield and J. L. Wayman [3] and J. Wayman, A. Jain, D. Maltoni, and D. Maio [4]. The former states that performance curves are very application, environment, and population dependent. Moreover, it contains an annex which details environmental factors and the corresponding affected biometric modality. The latter explains that changes in the application environment cause a significant impact on the biometric devices performance and also specifies a similar classification of the biometric applications than in [2]. Most recently books also refer to this problem: in

[5] T. Dunstone and N. Yager explained that one factor that affects biometric sample quality is environment. Likewise, many studies about different biometric modalities claimed the influence of environment in the capability of biometric capture devices to acquire biometric samples (e.g., [5] and [6]), in the quality of the acquired samples (e.g., [7, 8], and [9]), or in the overall biometric system performance (e.g., [6, 10], and [11]).

Considering all these previous works, environment must be considered as a relevant factor that can affect biometric performance negatively. In particular, it influences on the two main components involved in the first part of the recognition process: the biometric characteristic itself and the biometric capture device. These two elements are responsible for the adequate acquisition of biometric samples. If one of them, or even both of them, becomes influenced in its characteristics and behaves in an unexpected way, biometric samples may not be correctly acquired or their quality could be insufficient for an accurate performance of the whole biometric system. If such is the case, a consequence that may happen is that the level of security of the corresponding application may not be assured. Therefore, it is essential to quantify the influence of environment in biometric system performance.

Due to these circumstances, a new standard project was initiated in Working Group 5 – *Biometric Testing and Reporting* of ISO/IEC JTC1 SC37 [1] for the development of the ISO/IEC 29197 standard [12]. The purpose of this project was to establish the most appropriate methodology for measuring the environmental conditions influential effects on the performance of biometric systems.

The ISO/IEC 29197 Standard Overview

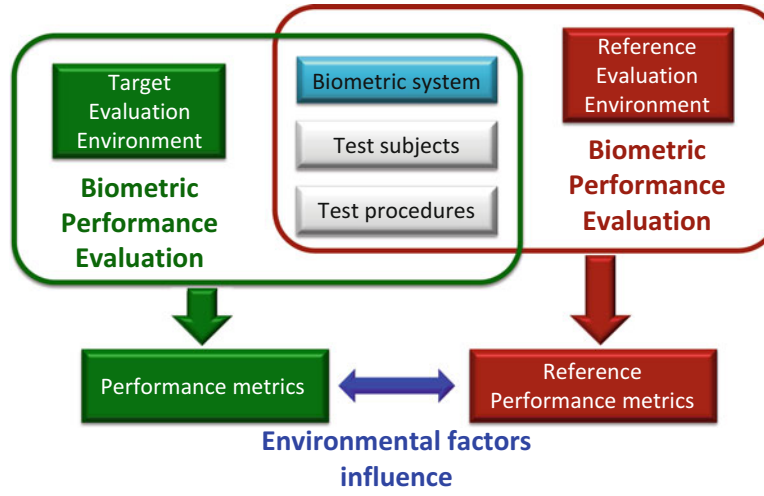
This standard provides a general evaluation methodology for analyzing and quantifying the environmental factors that influence on biometric performance. Specifically, the document (currently at the Draft International Standard stage (DIS)) covers the study of factors such as those atmosphere parameters (i.e., temperature, humidity, and atmospheric pressure) and other physical and chemical phenomena (i.e., illumination and noise) that can surround a biometric system during its operation. These factors can be real (naturally occurring) or modelled (artificially generated).

For carrying out these analyses, the defined evaluation methodology requires conducting a set of "end-to-end" biometric performance tests, in particular environmental conditions. Therefore, this standard is built upon the existing multipart standard ISO/IEC 19795 [13] for biometric performance testing and reporting (see ▶Performance Testing Methodology Standardization). In particular, the evaluation methodology considers two kinds of "end-to-end" biometric performance evaluations: scenario and operational testing. Scenario testing is a test intended for analyzing biometric systems in modelled environments considering a real-world target application and population. Alternatively, an operational testing is a test designed for testing biometric systems in real environments using a target population. Depending on the purpose of the evaluation, it will be appropriate to apply a different type of biometric performance evaluation. Usually, a modelled environment is a more controlled environment, unlike in a natural environment where there are many interacting factors in which control is not feasible. Consequently, scenario evaluations involve more precise tests, but operational evaluations are more realistic.

The following paragraphs describe the evaluation model addressed on the standard and summarize its major contents. At last, a brief description of some works carried out for supporting the development of the evaluation methodology is offered.

The ISO/IEC 29197 Evaluation Model

The evaluation model that has been established for environmental testing of biometric system



Environmental Testing Methodology of Biometric System Performance, Standardization, Fig. 1 Evaluation model for environmental testing of biometric system performance

performance is based on the comparison of performance measures obtained when both users and biometric systems are exposed to different environmental conditions. A diagram of this model can be seen in Fig. 1. Essentially, the model entails two types of biometric performance tests. One test shall be executed under reference environmental conditions which are the conditions for obtaining baseline performance data. These conditions are referred to as Reference Evaluation Environment (REE). The rest of the tests shall be executed under the different environmental conditions, the influence of which is going to be analyzed. Each group of these conditions is referred to as Target Evaluation Environments (TEEs). All the biometric performance tests carried out in either the REE or TEE are identical, including the same test subjects, following the same procedures, except for the environmental conditions values which are specific for each of the evaluation environments. As a consequence, from the results in each evaluation environment, it is possible to determine the biometric system performance for the corresponding environmental conditions. Moreover, the difference between the results of the REE and the TEEs allows knowing whether the biometric system is influenced, or not, by any environmental parameter, as well as quantifying this influence.

In addition, it is important to note that this evaluation model is suitable to analyze whether a single environmental parameter, or a combination of environmental parameters, can affect the biometric system performance. Also it is possible to deduct how the biometric system works in a particular environment compared to the same system working in a reference environment. Furthermore, this model allows tailoring the environmental conditions to assess according to the objectives of the evaluation. These objectives shall consider two major aspects: (a) based on the modality of the biometric system under test and the technology of the capture device, the environmental conditions of which are of interest to the study (e.g., temperature, humidity), and (b) based on the intended operational environment, the environmental specifications for the tested biometric system(s), and/or their possible extreme conditions, in which values of such environmental conditions shall be assessed.

The ISO/IEC 29197 Key Requirements

In view of the defined evaluation model, the standard covers two essential parts: the specification of the evaluation conditions and fundamental considerations for conducting scenario and

operational biometric performance tests as part of environmental testing evaluation.

Regarding the specification of evaluation conditions, the document addresses requirements to define the environmental conditions, to select the particular values to be analyzed, and to measure and record these conditions during the biometric performance tests. These requirements have been defined considering the type of evaluation environment (i.e., REE or TEE), the type of biometric performance evaluation (i.e., scenario and operational evaluation), and the relevant processes of a biometric system (i.e., enrolment or recognition).

In relation to biometric performance tests, the standard provides the necessary requirements to adapt scenario and operational biometric performance evaluations for environmental testing. The document addresses a special case of both types of tests. For scenario evaluations, this is based on ISO/IEC 19795-2 [14], whereas for operational evaluations, this is based on ISO/IEC 19795-6 [15].

Moreover, the standard contains two informative annexes. The first one offers recommendations for the selection of the environmental conditions values. The second annex presents additional information related to the proper test equipment and its functionality.

Preliminary Environmental Testing Evaluations

During the development of the ISO/IEC 29197 evaluation methodology, some experiments have been conducted for completing and improving it. One of them was carried out to study which environmental conditions influence on a vascular biometric technology [6]. That evaluation involved the analysis of three environmental conditions (i.e., temperature, humidity, and illumination) carrying out biometric performance scenario tests. For doing that, eight scenarios were defined considering different values of temperature (i.e., high, cool, and cold temperatures), illumination (i.e., fluorescent lighting, incandescent lighting, sunlight, and darkness), and humidity (high relative humidity) in addition to a reference scenario. Results of this evaluation showed that the FMR rate was not affected, but the FTA and FNMR rates increase considerably when the vascular biometric system has to work under illumination conditions that entail high levels of infrared light.

Another important experiment was performed for analyzing a fingerprint biometric systems working in a typical hot humid environment (i.e., 40 °C ± 2 °C of temperature and 60 % ± 5 % of relative humidity) in comparison to the common environment of a laboratory (i.e., 26 °C ± 2 °C of temperature and 40 % ± 5 % of relative humidity) [16]. In this evaluation, two environmental conditions were assessed: temperature and relative humidity, and one environmental condition was controlled, illumination. Two evaluation environments were established: a REE for testing the laboratory conditions and a TEE for analyzing the hot humid environmental conditions. In each environment a biometric performance scenario evaluation was executed. The TEE environmental conditions were generated using a climatic chamber. Performance results revealed that the recognition capability of this biometric system was not affected by the conditions of the tested hot humid environment.

A more detailed explanation about the aforementioned experiments and the development of the evaluation methodology is offered in Chap. 5 of [17].

Summary

Environment is one of the most important factors that could affect biometric performance negatively. These effects can be quantified by means of environmental testing. This is a kind of biometric performance evaluations in which the influence of environmental factors on biometric performance is studied. The ISO/IEC 29197 standard [1] establishes a generic evaluation methodology for conducting these kinds of tests. This methodology includes requirements to specify the environmental conditions to analyze and to carry out biometric performance tests.

Related Entries

- Influential Factors to Performance
- Performance Evaluation, Overview
- Performance Measures
- Performance Testing Methodology Standardization

References

1. ISO/IEC Joint Technical Committee 1, Subcommittee 37 – Biometrics, http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home/jtc1_sc37_home.htm
2. A. Jain, R. Bolle, S. Pakanti, *Biometrics: Personal Identification in Networked Society* (Kluwer Academic, Boston, 1999)
3. A.J. Mansfield, J.L. Wayman, Best practices in testing and reporting performance of biometric devices. Version 2.01, Centre for Mathematics and Scientific Computing, National Physical Laboratory, 200
4. J. Wayman, A. Jain, D. Maltoni, D. Maio, *Biometric Systems: Technology, Design and Performance Evaluation* (Springer, London, 2005)
5. T. Dunstone, N. Yager, *Biometric System and Data Analysis, Design, Evaluation, and Data Mining* (Springer, New York, 2009)
6. R. Sanchez-Reillo, B. Fernandez-Saavedra, J. Liu-Jimenez, Y.B. Know, Changes to vascular biometric system security & performance. IEEE Trans. Aerosp. Electron. Syst. Mag. **24**(6), 4–14
7. H. Kim, Evaluation of fingerprint readers: environmental factors, human factors, and liveness detecting capability, http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/Microsoft%20PowerPoint%20-%20Presentation%20of%20HaleKim%20-%20v2.1.ppt%20%5B.pdf
8. H. Kang, B. Lee, H. Kim, D. Shin, J. Kim, A study of performance evaluation of fingerprint sensors, audio- and video-based biometric person authentication. Lect. Notes Comput. Sci. **2688**, 574–583 (2003)
9. H. Proença, Quality assessment of degraded iris images acquired in the visible wavelength. IEEE Trans. Inf. Forensics Secur. **6**(1), 82–95 (2011)
10. E. Kukula, S. Elliott, R. Waupotitsch, B. Pesenti, Effects of illumination changes on the performance of Geometrix FaceVision 3D FRS, in *38th Annual International Carnahan Conference on Security Technology*, Albuquerque, 2004, pp. 331–337
11. J.R. Beveridge, D.S. Bolme, B.A. Draper, G.H. Givens, L. Yui Man, P.J. Phillips, Quantifying how lighting and focus affect face recognition performance, in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, San Francisco, 2010, pp. 74–81
12. ISO/IEC DIS 29197, Information technology – Evaluation methodology for environmental influence in biometric system performance, 2013
13. ISO/IEC 19795, Information technology – Biometric testing and reporting (multipart standard). Published standards available at http://www.iso.org/iso/home/store.htm
14. ISO/IEC 19795-2:2007, Information technology – Biometric performance testing and reporting – Part 2: testing methodologies for technology and scenario evaluation (2007), available at http://www.iso.org/iso/home/store.htm
15. ISO/IEC 19795-6:2012, Information technology – Biometric performance testing and reporting – Part 6: testing methodologies for operational evaluation (2012), available at http://www.iso.org/iso/home/store.htm
16. B. Fernandez-Saavedra, F.J. Diez-Jimeno, R. Sanchez-Reillo, R. Lazarick, Establishment of baseline performance for "end to end" biometric system evaluations, in *2010 IEEE International Carnahan Conference on Security Technology (ICCST)*, San Jose, 5–8 Oct 2010, pp. 330, 335
17. B. Fernandez, Evaluation methodologies for security testing biometric systems beyond technological evaluation. PhD thesis, Electronic Technology Department, Carlos III University of Madrid, 2013

Ergonomic Design for Biometric Systems

Eric P. Kukula[1] and Stephen John Elliott[2]
[1]Department of Industrial Technology, Purdue University, West Lafayette, IN, USA
[2]International Center for Biometric Research, Purdue University, West Lafayette, IN, USA

Synonyms

Human-Biometric Sensor Interaction (HBSI); Human-Computer Interaction (HCI); Human Factors; Usability

Definition

Biometric ergonomic design is the area of research that examines how humans interact with and use biometric sensors, devices, interfaces, and systems. The purpose is to understand the

physical and cognitive human-biometric sensor interaction to improve the system design and overall performance of a biometric system.

Introduction

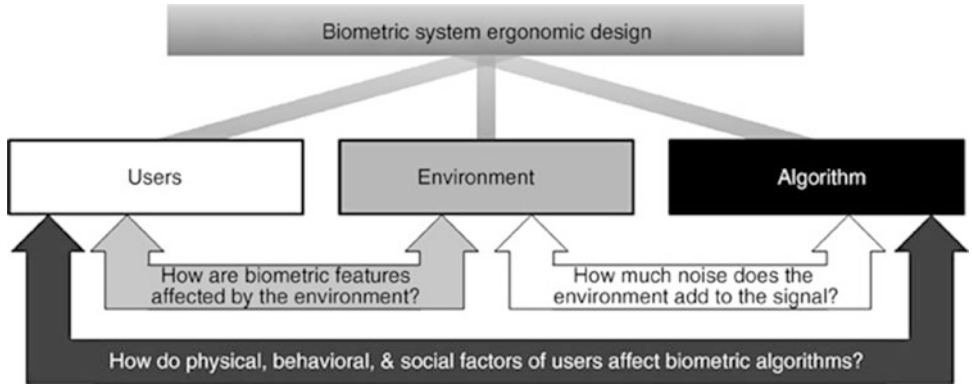
Biometric ergonomic design is an emerging interdisciplinary research area in biometrics that focuses on the interaction between the user and the biometric system to better understand issues and errors, users knowingly or unknowingly generate when attempting to use a biometric system. This research area attempts to understand what tasks, movements, and behaviors users execute when encountering different biometric modalities. This area presents a challenge for the biometrics community - while the algorithms are continually improving, there are still individuals who cannot successfully interact with the biometric sensor(s). It is essential that designers continue examining biometric devices, processes, or systems to ensure they accommodate the focal point of any biometric systems, *the human*. Adapting devices, processes or systems to the *human* can increase usability by minimizing errors during presentation and acquisition of the biometric characteristics to the sensor through better design, instruction, or system feedback.

Traditional approaches to evaluate the performance of a biometric system have been system-level, meaning that evaluators and designers are more interested in system-reported error rates, some of which include the *failure to enroll (FTE)* rate, failure to acquire *(FTA) rate*, *false accept rate* (FAR), and *false reject rate (FRR)*. Traditional performance evaluations have worked well to evaluate emerging technologies, new biometric modalities, and algorithm revisions, which are typically associated with *technology performance evaluations*. Moreover, since biometrics entered the commercial marketplace, most research has been dedicated to the development in three areas: (1) improving performance, (2) increasing throughput, and (3) decreasing the size of the sensor or hardware device. Limited research has focused on ergonomic design and usability issues, which relate to how users interact and use biometric devices. No standard activities have focused on ergonomic design or usability issues with biometrics, although standard testing and evaluation protocols do exist, specifically – ISO 19795-1: Technology Testing [1], ISO 19795-2: Scenario Testing [2], and ISO TR19795-3: Modality-Specific Testing [3].

While early research has been concerned with the design, development, and testing of biometric systems and algorithms, recent research has attributed human physical, behavioral, and social factors to affect the performance of the overall biometric system. Moreover, these factors are of utmost importance when conducting *scenario* and *operational performance evaluations*, as they are the last line of defense between the laboratory and the commercial marketplace to understand how a biometric system performs in a particular environment or with a specific set of users. Therefore, as the community continues to learn more about the different biometric modalities and systems, as well as how users interact with them, performance from both the system and user perspectives must be fully understood to make further improvements to the biometric sensor, algorithm, and design of future user interfaces.

Biometric Properties and Ergonomic Implications

Biometric modalities are classified as physiological, behavioral, or a combination of the two. In addition, they are classified according to five desirable properties, outlined by Clarke [4] and amended by numerous others. Desirable properties of biometric characteristics are that they offer (1) universality – available to all people, (2) invariant – features extracted are nonchanging, (3) high intraclass variability – features extracted are distinct for each user; (4) acceptability – characteristic of suitability for use by everyone, and (5) extractability – a sensor can extract the features presented in a repeatable manner. Although commonly described in the literature as



Ergonomic Design for Biometric Systems, Fig. 1 Issues that affect biometric system performance and the relationship with ergonomics

the ideal characteristics of the biometric, each must overcome challenges. Herein lies one of the challenges associated with large-scale deployment of biometrics and the purpose behind research in this area – the majority of biometrics are challenged to satisfy all these five categories.

To better understand the importance of ergonomics in biometrics, the authors pose the question: *What affects biometric system performance*? Generalizing the issues that can be linked to many performance failures into three divisions, bins for users (physical, behavioral, and social factors), the environment, and matching algorithms emerge. While it is important to understand each group when designing a biometric system, the inter-relationship between the groups also impacts biometric performance, which is illustrated in Fig. 1. First, the user-environment relationship impacts performance. For example, climatic or work conditions may require individuals to wear personal protective equipment (PPE), which not only limits biometric modalities that can be deployed but may also occlude the biometric characteristics from being successfully acquired in the first place, such as the case in safety glasses for iris recognition. In addition, atmospheric conditions such as temperature and humidity can impact the skin, affecting the acquisition for some modalities. Second is the environment and inter-relationship of algorithms. Examples of this include ambient noise for voice recognition and illumination or busy backgrounds for face recognition. Third is the relationship between users and algorithms. First, physiological factors such as skin moisture, elasticity, age, and color can affect performance of algorithms. Secondly, behavioral factors such as finger preference can impact performance. For example, individuals of Asian descent prefer to use the little finger for fingerprint recognition, but it is documented in the literature [5, 6] that the little finger is the worst-performing finger. Lastly, social preferences or factors such as hair length or the wearing of head coverings can impact face and iris recognition due to the occlusion of necessary features. While the literature has investigated some of the aforementioned items, more research is needed in these areas. However, there is also an interaction between the three clusters as indicated in the research conducted by Kukula et al. [7, 8], but it has not been thoroughly investigated.

It is well documented in the literature that image quality affects the biometric matching algorithm. Yao et al. [9] stated that "in a deployed system, the poor acquisition of samples perhaps constitutes the single most important reason for high false reject/accept rates" and further discussed that there are two solutions for reducing poor images. First, one can model and weigh all adverse situations for the feature extraction and matching system. Second, "one can try to dynamically and interactively obtain a desirable input sample." Improving the ergonomic design of biometric systems is one method to dynamically "modify" the input sample through im-

proved usability of biometric devices, processes, and systems.

Common Design Concerns

Biometric systems are heavily dependent on the sensor to acquire the sample, segment it, and extract features from samples for the matcher to determine the correct response. By observing how users interact with biometric sensors, several design issues are apparent but could be resolved by integrating knowledge of industrial design, ergonomics and human factors, and usability. Rubin [10] discusses five reasons why products and systems are difficult to use. The main problem is that the emphasis and focus has been on the machine/system and not on the end user during development. Common design misconceptions are

- Humans are flexible and will adjust to a product or device.
- Engineers work well with technology but not with people.
- Engineers are hired to solve technology problems and not people skills.
- Designers create products for users like themselves in terms of both usage and level of knowledge [10].

The following factors are true within the context of biometric system design. Humans will adapt to the sensor and/or system. Many times, biometric systems or sensors are not tested on sufficiently large numbers of the general populations, namely, due to the cost of doing so. Moreover, the biometric community may test the algorithms exhaustively offline, using precollected images, but lapse on collecting images with a new sensor to examine how the user interacts with the system or device.

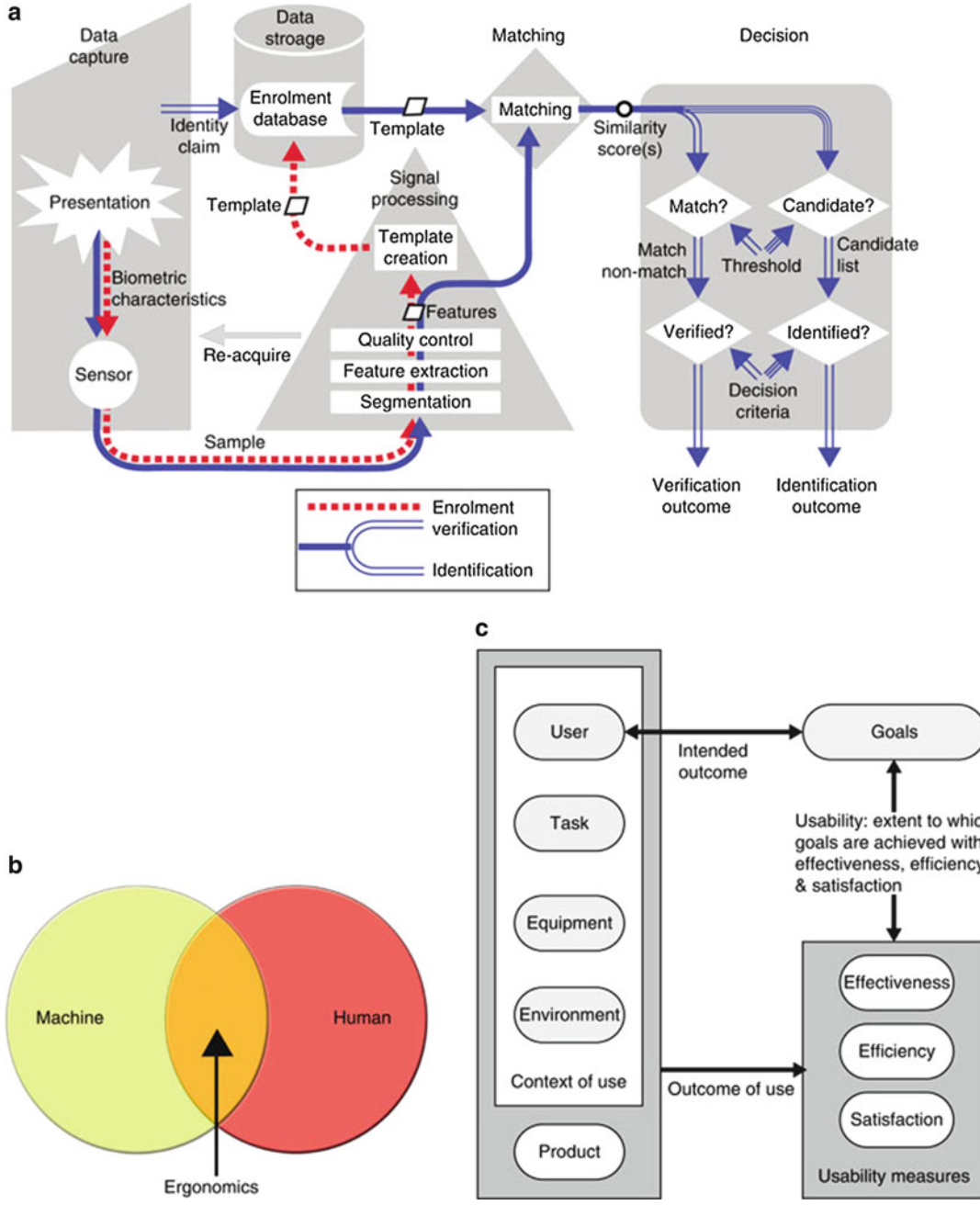
According to Smith [11], some members of the Human-Computer Interaction (HCI) community believe that interfaces of security systems do not reflect good thinking in terms of creating a system that is easy to use, while maintaining an acceptable level of security (p. 75). Moreover, according to Adams and Sasse [12], security systems are one of the last areas to embrace user-centered design and training as essential. This is also true for biometrics as Coventry et al. [13] stated the Human-Computer Interaction (HCI) community has had limited involvement in the design or evaluation of biometric systems.

Human-Biometric Sensor Interaction (HBSI)

The authors have been researching this area for over 4 years. Results of this research have produced a new conceptual model, which is shown in Fig. 2. This model combines literature and models from biometrics, ergonomics, and usability (Fig. 3). The conceptual model that examines biometric system ergonomic design is called the human-biometric sensor interaction, or HBSI. The three fields of biometrics, ergonomics, and usability are arranged within the model to show the relationship of the human, biometric sensor, and the biometric system. Each of the relationships poses a different set of design or research questions, which will now be discussed.

Human-Biometric Sensor

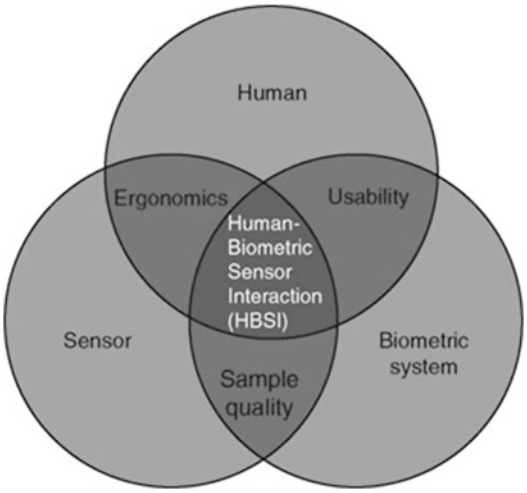
The human and sensor components of the HBSI model are similar to Tayyari and Smith's [14] human-machine interaction model. Much like the traditional model, the human and biometric sensor components look to achieve the optimal relationship between humans and a biometric sensor in a particular environment. The human-biometric sensor relationship parallels the presentation silo of the general biometric model and is often overlooked during the design of the biometric system. Applying an ergonomic approach during the design of the biometric sensor, we can fit the sensors to the majority of users, as opposed to forcing users to interact with difficult and uncomfortable biometric sensors. Applying ergonomic approaches such as user-centered design, biometric sensors, interfaces, and systems can be designed based on the user's physical and mental states to allow the users to complete the task that the biometric system is asking for most efficiently.



Ergonomic Design for Biometric Systems, Fig. 2 General biometric model (**a**) [1], general ergonomic model (**b**) [14], and general usability model (**c**) [15].

Human-Biometric System

The human and biometric system components of the HBSI model are arranged to accommodate the way that biometric sensors, software, and implementations are presented to users. Not only a biometric sensor must be designed so that a user can interact with it in a repeatable fashion but also the sensor(s), software, and the way the entire "system" is packaged must be usable. Usability



Ergonomic Design for Biometric Systems, Fig. 3 The human-biometric sensor interaction or HBSI model

according to ISO 9241-11 [15] is segmented into three factors: effectiveness, efficiency, and satisfaction. Each of the three metrics is distinctively different and important to understand. System designers must take into consideration the goals of the system. Every biometric system will be designed for a different purpose; thus, a balance must be attained between effectiveness, efficiency, and satisfaction. First, biometric systems must be effective, meaning users are able to interact, use, and complete the desired tasks without too much effort, which can also cause throughput issues if people get "lost" in the system and require administrator intervention, which also comes with a cost. Second, biometric systems must be efficient, meaning users must be able to accomplish the tasks easily and in a timely manner. Again, if users require intervention, the cost of staffing becomes burdensome. Third, users must like, or be satisfied with, the biometric system or will discontinue use and find alternative methods to accomplish the task.

Sensor-Biometric System

As mentioned in the previous two sections, users must be able to interact with a biometric sensor or device in a consistent manner over time; however, users must also find the entire biometric system usable. To enable this, the third relationship of the HBSI conceptual model emerges, i.e., the sensor-biometric system measured by image quality. Image quality is the important link between these two components because the image or sample acquired by the biometric sensor must contain the characteristics or features needed by the biometric system to enroll or match a user in the biometric system. So not only does the human-sensor relationship need to be functional and the human-biometric system need to be usable but also the sensor-biometric system needs to be efficient. This occurs only if the sensor captures and passes usable features onto the biometric system.

The Human-Biometric Sensor Interaction

The combination of components and relationships in the model form the human-biometric sensor interaction. Each component that is in the HBSI model has been shown to impact results in previous experiments from the respective field from which it was adapted Since the conceptual model is derived from different fields, each component usability, ergonomics, and biometrics produces a unique output. Thus, the final determination of the results is dependent upon the goals, objectives, and criteria the researcher, designer, or engineer is seeking, which is in line with the ergonomics, usability, and design literature. As work in the area of biometric system ergonomic design is limited, the HBSI model provides the biometrics community more insight and considerations needed for designing biometric systems and their corresponding devices, as well as metrics to evaluate the components outside traditional biometric testing and evaluation.

Literature

Seminal research and publication in the area of usability and accessibility, which was concerned with biometric system ergonomic design, were

pioneered by the User Research Group at National Cash Register (NCR). Some of their research findings that would impact biometric system design can be seen in the results of one experiment, which revealed that successful verification was not affected by the type of instruction and feedback received. Furthermore, the results also revealed some users have problems that cannot be solved through instruction, training, or feedback. A possible explanation could be the biometric system ergonomic design and placement of the sensor and the human-biometric sensor interaction. Please refer to a book chapter written by Coventry [16] for more information and relevant citations of work conducted by the User Research Group at NCR.

Two other groups that have been actively researching and publishing in this area are the NIST Biometrics and Usability Group [17] and Purdue University's Biometric Standards, Performance, & Assurance Laboratory [18]. Please refer to the respective references for the latest research, publications, and presentations in the area of biometric system ergonomic design. At the time of writing, research in this area has investigated tenprint fingerprint capture scanner height and angle, hand geometry device height, habituation, applied finger force on a fingerprint sensor, and usability of small-area and swipe-based fingerprint sensors, image quality evaluations, instruction and feedback mechanisms, as well as health and safety perceptions of biometric devices. Lastly, the United Kingdom Home Office Identity and Passport Service has also published reports based on their biometric trials and implementations which discuss biometric usability and ergonomic design [19]. Maple and Norrington [20] reported one particular trial of the United Kingdom's Passport Service Trial Program and its usability and found issues with each of the three evaluated biometric systems: fingerprint, face, and iris recognition systems.

Summary

This entry discussed the effect human interaction has on biometric system performance to outline the impact biometric system ergonomic design can have on the overall performance of a biometric system. The entry has outlined the origins of the human-biometric sensor interaction model including relevant work and models in the fields of ergonomics, user-centered design, usability, and HCI. In addition, this entry has discussed how the fields that form the HBSI model not only relate to biometrics but can be integrated into the design of biometric devices and systems to create more usable devices and systems with the goal of lowering acquisition, enrollment, and matching failures. However, further understanding in the area of biometric system ergonomic design and its impact on biometrics is needed to meet this goal.

The authors are not alone in their thoughts and opinions that continued research is needed in the area of biometric system ergonomic design. Smith [11] stated that some members of the HCI community believe that interfaces of security systems do not reflect good thinking in terms of creating a system that is easy to use, while maintaining an acceptable level of security. Moreover, Adams and Sasse discussed the fact that security systems are one of the last areas to embrace user-centered design and training as essential [12]. Lastly, Maple and Norrington [20] noted three observations that align with the objective for continued investigation in biometric system ergonomic design:

- People have different cognitive abilities.
- People have different physical characteristics and interact differently with equipment.
- People have different sensory abilities and will perceive biometric sensors and systems differently.

As the biometrics community continues to develop biometric systems and deployments become more pervasive, the evaluation of the biometric system and the respective human-biometric sensor interaction will continue to gain traction.

Related Entries

▸ Biometric System Design, Overview

▸ User Acceptance
▸ User Interface, System Design

References

1. International Standards Organization, Information technology – biometric performance testing and reporting – Part 1: principles and framework (ISO/IEC, Geneva, 2006), p. 56
2. International Standards Organization, Information technology – biometric performance testing and reporting – Part 2: testing methodologies for technology and scenario evaluation (ISO/IEC, Geneva, 2007), p. 48
3. International standards organization, Text of DTR 19795-3, Biometric performance testing and reporting – Part 3: modality-specific testing (ISO/IEC, Geneva, 2007), p. 28
4. R. Clarke, Human identification in information systems: management challenges and public policy issues. Inf. Technol. People **7**(4), 6–37 (1994)
5. M. Young, S. Elliott, Image quality and performance based on Henry classification and finger location, in *IEEE Workshop on Automatic Identification Advanced Technologies*, Alghero, 2007
6. J. Wayman, Multi-finger penetration rate and ROC variability for automatic fingerprint identification systems, in *National Biometric Test Center Collected Works 1997–2000*, ed. by J. Wayman (Office of Research and Graduate Studies and the College of Engineering/San Jose State University, San Jose, 2000), pp. 179–190
7. E. Kukula, Design and evaluation of the human-biometric sensor interaction method, in *Industrial Technology*, vol. 1, Ph.D. (Purdue University, West Lafayette, 2008), p. 510
8. E. Kukula, S. Elliott, V. Duffy, The effects of human interaction on biometric system performance, in *12th International Conference on Human-Computer Interaction and 1st International Conference on Digital-Human Modeling*, Beijing (Springer, 2007), pp. 903–913
9. M. Yao, S. Pankanti, N. Haas, Fingerprint quality assessment, in *Automatic Fingerprint Recognition Systems*, ed. by N. Ratha, R. Bolle (Springer, New York, 2004), pp. 55–66
10. R. Rubin, *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests* (Wiley, New York, 1994)
11. S. Smith, Humans in the loop: human-computer interaction and security. IEEE Secur. Priv. **1**(3), 75–79 (2003)
12. A. Adams, M. Sasse, Users are not the enemy: why users compromise security mechanisms and how to take remedial measures. Commun. ACM **42**(12), 41–46 (1999)
13. L. Coventry, A. De Angeli, G. Johnson, Usability and biometric verification at the ATM interface, in *Conference on Human Factors in Computing Systems* (ACM Press, Ft. Lauderdale, 2003)
14. F. Tayyari, J. Smith, Occupational ergonomics: principles and applications, in *Manufacturing Systems Engineering Series*, ed. by H. Parsaei (Kluwer Academic, Norwell, 2003), p. 452
15. International Organization for Standardization, ISO 9241: ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: guidance on usability (1998), p. 28
16. L. Coventry, Usable biometrics, in *Security and Usability: Designing Secure Systems that People Can Use*, ed. by L.F. Cranor, S. Garfinkel (O'Reilly Media, Sebastopol, 2005), pp. 175–198
17. NIST. Biometrics and usability group (2007). Available from http://zing.ncsl.nist.gov/biousa/index.html. Accessed 30 Nov 2007
18. Purdue University Biometric Standards Performance & Assurance Laboratory, Human biometric sensor interaction. 2007 [cited 2007 Nov 30], Available from http://www.bspalabs.org/archives/category/research/hbsi
19. Home Office Identity & Passport Service. Publications (2007). Available from http://www.ips.gov.uk/passport/publications-general.asp. Accessed 30 Nov 2007
20. C. Maple, P. Norrington, The usability and practicality of biometric authentication in the workplace, in *IEEE First International Conference on Availability, Reliability and Security (ARES'06)*, Vienna, 2006

Eye Features and Anatomy

Kristina Irsch and David L. Guyton
The Wilmer Ophthalmological Institute, The Johns Hopkins University School of Medicine, Baltimore, MD, USA

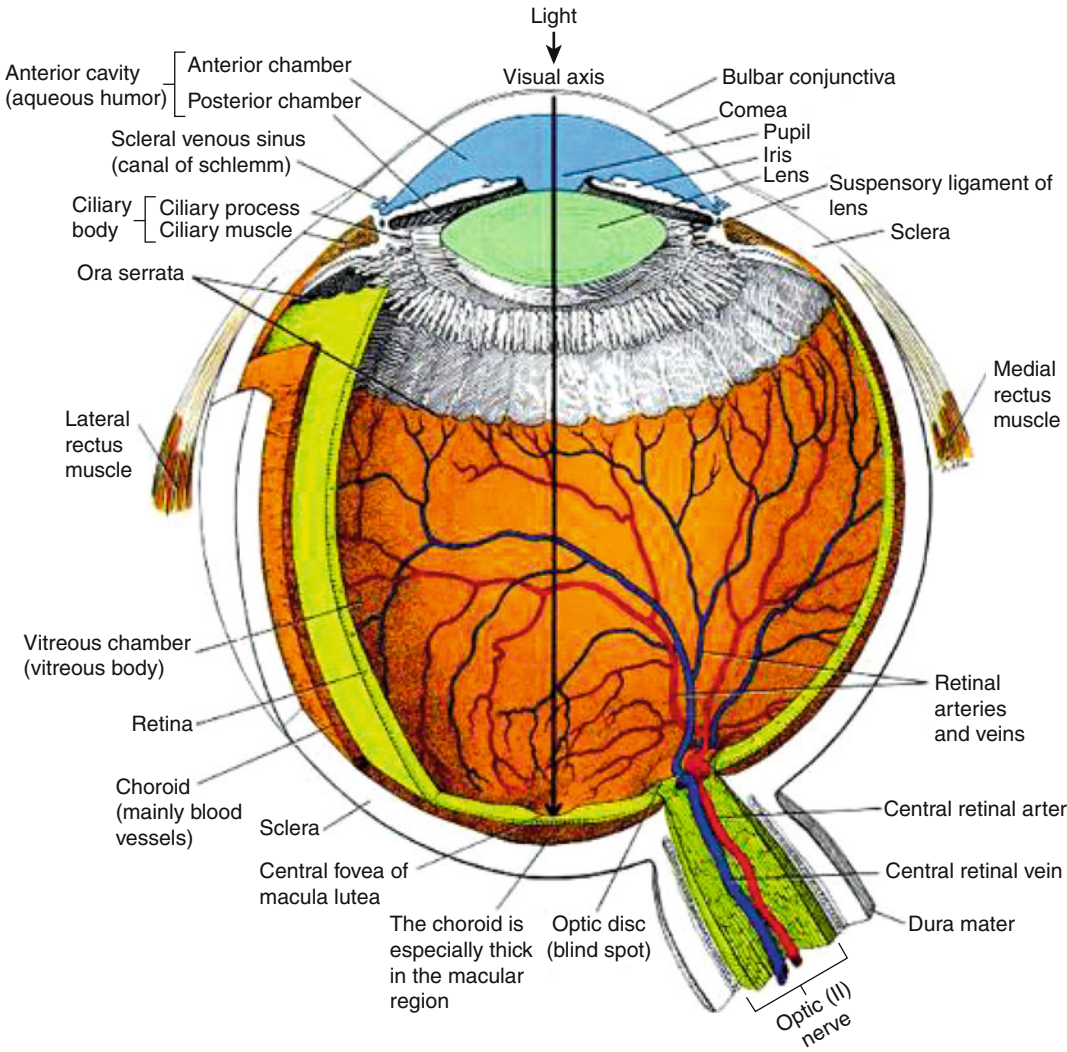
Definition

The human eye is one of the most remarkable sensory systems. Leonardo da Vinci was acutely aware of its prime significance: "The eye, which is termed the window of the soul, is the chief organ whereby the *senso comune* can have the most complete and magnificent view of the infinite works of nature" [1]. The human being

gathers most of its information on the external environment by its eyes and thus relies on sight more than on any other sense, with the eye being the most sensitive organ that we have. Besides its consideration as a window to the soul, the eye can indeed serve as a window to the identity of an individual. It offers unique features for the application of identification technology. Both the highly detailed texture of the iris and the fundus blood vessel pattern are unique to every person, providing suitable traits for biometric recognition.

Anatomy of the Human Eye

The adult eyeball, often referred to as a spherical globe, is only approximately spherical in shape, with its largest diameter being 24 mm anteroposteriorly [2, 3]. A schematic drawing of the human eye is shown in Fig. 1. The anterior portion of the eye consists of the cornea, iris, pupil, and crystalline lens. The pupil serves as an aperture which is adjusted by the surrounding **iris**, acting as a diaphragm that regulates the amount of light entering the eye. Both the iris and



Eye Features and Anatomy, Fig. 1 Schematic drawing of the human eye [4]

the pupil are covered by the convex transparent cornea, the major refractive component of the eye due to the huge difference in refractive index across the air-cornea interface [5]. Together with the crystalline lens, the cornea is responsible for the formation of the optical image on the retina. The crystalline lens is held in place by suspensory ligaments, or zonules, that are attached to the ciliary muscle. Ciliary muscle actions cause the zonular fibers to relax or tighten and thus provide accommodation, the active function of the crystalline lens. This ability to change its curvature, allowing objects at various distances to be brought into sharp focus on the retinal surface, decreases with age, with the eye becoming "presbyopic." Besides the cornea and crystalline lens, both the vitreous and aqueous humor contribute to the dioptric apparatus of the eye, leading to an overall refractive power of about 60 diopters [3]. The aqueous humor fills the anterior chamber between the cornea and iris and also fills the posterior chamber that is situated between the iris and the zonular fibers and crystalline lens. Together with the vitreous humor, or vitreous, a loose gel filling the cavity between the crystalline lens and retina, the aqueous humor is responsible for maintaining the intraocular pressure and thereby helps the eyeball maintain its shape. Moreover, this clear watery fluid nourishes the cornea and crystalline lens. Taken all together, with its refracting constituents, self-adjusting aperture, and last but not least its detecting segment, the eye is very similar to a photographic camera. The film of this optical system is the **retina**, the multilayered sensory tissue of the posterior eyeball onto which the light entering the eye is focused, forming a reversed and inverted image. External to the retina is the *choroid*, the layer that lies between retina and sclera. The choroid is primarily composed of a dense capillary plexus, as well as small arteries and veins [5]. As it consists of numerous blood vessels and thus contains many blood cells, the choroid supplies most of the back of the eye with necessary oxygen and nutrients. The sclera is the external fibrous covering of the eye. The visible portion of the sclera is commonly known as the "white" of the eye.

Both the iris and retina are described in more detail in the following sections due to their major role in biometric applications.

Iris

The iris may be considered as being composed of four different layers [3], starting from anterior to posterior: (i) *the anterior border layer* which mainly consists of fibroblasts and pigmented melanocytes, interrupted by large, pit-like holes, the so-called crypts of Fuchs; (ii) S*troma* containing loosely arranged collagen fibers that are condensed around blood vessels and nerve fibers. Besides fibroblasts and melanocytes, as present in the previous layer, clump cells and mast cells are found in the iris stroma. It is the pigment in the melanocytes that determines the color of the iris, with blue eyes representing a lack of melanin pigment. The *sphincter pupillae muscle*, whose muscle fibers encircle the pupillary margin, lies deep inside the stromal layer. By contracting, the sphincter causes pupil constriction, which subsequently results in the so-called contraction furrows in the iris. These furrows deepen with dilation of the pupil, caused by action of the dilator muscle, which is formed by the cellular processes of the (iii) *anterior epithelium*. The dilator pupillae muscle belongs to the anterior epithelial layer, with its cells being myoepithelial [6]. Unlike the sphincter muscle, the muscle fibers of the dilator muscle are arranged in a radial pattern, terminating at the iris root; and (iv) finally the *posterior pigmented epithelium* whose cells are columnar and more heavily pigmented in comparison with the anterior epithelial cells. The posterior epithelial layer functions as the main light absorber within the iris.

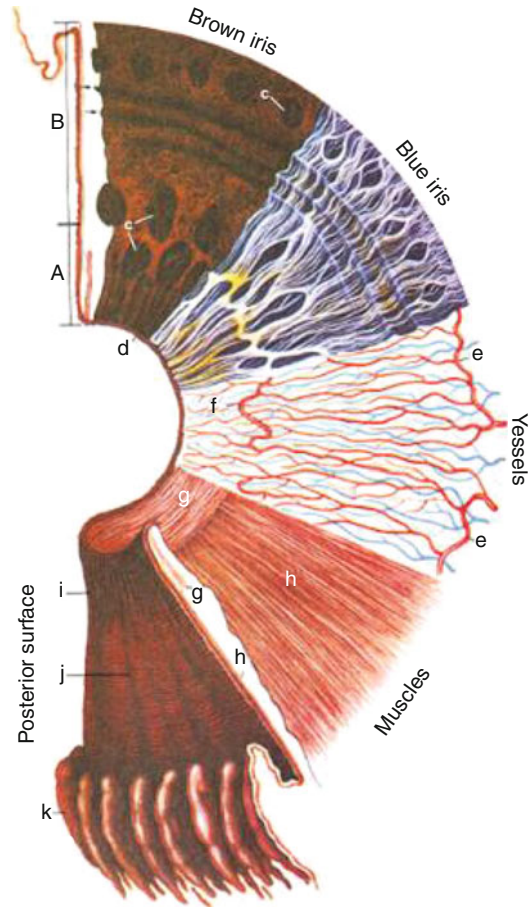
A composite view of the iris surfaces and layers is shown in Fig. 2, which indicates the externally visible iris features, enhancing the difference in appearance between light and dark irides. Light irides show more striking features in visible light because of higher contrast. But melanin is relatively transparent to near-infrared light, so viewing the iris with light in the near-infrared range will uncover deeper features arising from

the posterior layers and thereby reveals even the texture of dark irides that is often hidden with visible light.

In general, the iris surface is divided into an inner pupillary zone and an outer ciliary zone. The border between these areas is marked by a sinuous structure, the so-called collarette. In addition to the particular arrangement of the iris crypts themselves, the structural features of the iris fall into two categories [7]: (i) features that relate to the pigmentation of the iris (e.g., pigment spots, pigment frill) and (ii) movement-related features, in other words features of the iris relating to its function as pupil size control (e.g., iris sphincter, contraction furrows, radial furrows).

Among the visible features that relate to pigmentation belong small elevated white or yellowish Wölfflin spots in the peripheral iris, which are predominantly seen in light irides [3]. The front of the iris may also reveal iris freckles, representing random accumulations of melanocytes in the anterior border layer. Pigment frill or pupillary ruff is a dark pigmented ring at the pupil margin, resulting from a forward extension of the posterior epithelial layer. In addition to the crypts of Fuchs, predominantly occurring adjacent to the collarette, smaller crypts are located in the periphery of the iris. These depressions, which are dark in appearance because of the darkly pigmented posterior layers, are best seen in blue irides. Similarly, a buff-colored, flat, circular strap-like muscle becomes apparent in light eyes, that is, the iris sphincter. The contraction furrows produced when it contracts, however, are best noticeable in dark irides, as the base of those concentric lines is less pigmented. They appear near the outer part of the ciliary zone and are crossed by radial furrows occurring in the same region. Posterior surface features of the iris comprise structural and circular furrows, pits, and contraction folds. The latter, for instance, also known as Schwalbe's contraction folds, cause the notched appearance of the pupillary margin.

All of the features described above contribute to a highly detailed iris pattern that varies from one person to the next. Even in the same individual, right and left irides are different in texture. Besides its uniqueness, the iris is a protected but



Eye Features and Anatomy, Fig. 2 Composite view of the surfaces and layers of the iris. Crypts of Fuchs (*c*) are seen adjacent to the collarette in both the pupillary (*A*) and ciliary zone (*B*). Several smaller crypts occur at the iris periphery. *Two arrows* (top left) indicate circular contraction furrows occurring in the ciliary area. The pupillary ruff (*d*) appears at the margin of the pupil, adjacent to which the circular arrangement of the sphincter muscle (*g*) is shown. The muscle fibers of the dilator (*h*) are arranged in a radial fashion. The last sector at the bottom shows the posterior surface with its radial folds (*i* and *j*) (Reproduced with permission from [5])

readily visible internal organ, and it is essentially stable over time [7, 8]. Thus the iris pattern provides a suitable physical trait to distinguish one person from another. The idea of using the iris for biometric identification was originally proposed by the ophthalmologist Burch in 1936 [9]. However, it took several decades until two other ophthalmologists, Flom and Safir [7], patented the general concept of iris-based recognition.

In 1989, Daugman, a mathematician, developed efficient algorithms for their system [8–10]. His mathematical formulation provides the basis for all iris scanners now in use. Current iris recognition systems use infrared-sensitive video cameras to acquire a digitized image of the human eye with near-infrared illumination in the 700–900 nm range. Then, image analysis algorithms extract and encode the iris features into a binary code which is stored as a template. Elastic deformations associated with pupil size changes are compensated for mathematically. As pupil motion is limited to living irides, small distortions are even favorable by providing a control against fraudulent artificial irides [8, 10].

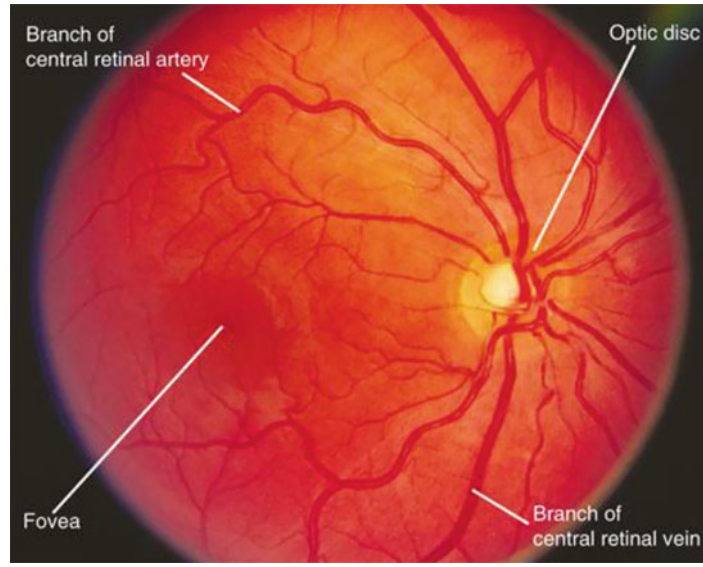
Imaging the iris with near-infrared light not only greatly improves identification in individuals with very dark, highly pigmented irides, but also makes the system relatively immune to anomalous features related to changes in pigmentation. For instance, melanomas/tumors may develop on the iris and change its appearance. Furthermore, some eye drops for glaucoma treatment may affect the pigmentation of the iris, leading to coloration changes or pigment spots. However, as melanin is relatively transparent to near-infrared light and basically invisible to monochromatic cameras employed by current techniques of iris recognition, none of these pigment-related effects causes significant interference [9, 10].

Retina

As seen in an ordinary histologic cross section, the retina is composed of distinct layers. The retinal layers from the vitreous to choroid [2, 3] are the (i) *internal limiting membrane*, formed by both retinal and vitreal elements [2], and the (ii) *nerve fiber layer*, which contains the axons of the ganglion cells. These nerve fibers are bundled together and converge to the optic disc, where they leave the eye as the optic nerve. The cell bodies of the ganglion cells are situated in the (iii) *ganglion cell layer*. Numerous dendrites extend into the (iv) *inner plexiform layer* where they form synapses with interconnecting cells, whose cell bodies are located in the (v) *inner nuclear layer*; (vi) *outer plexiform layer*, containing synaptic connections of photoreceptor cells; (vii) *outer nuclear layer*, where the cell bodies of the photoreceptors are located; (viii) *external limiting membrane*, which is not a membrane in the proper sense, but rather comprises closely packed junctions between photoreceptors and supporting cells. The photoreceptors reside in the (ix) *receptor layer*. They comprise two types of receptors: rods and cones. In each human retina, there are 110–125 million rods and 6.3–6.8 million cones [2]. Light contacting the photoreceptors and thereby their light-sensitive photopigments is absorbed and transformed into electrical impulses that are conducted and further relayed to the brain via the optic nerve; and finally the (x) *retinal pigment epithelium*, whose cells supply the photoreceptors with nutrients. The retinal pigment epithelial cells contain granules of melanin pigment that enhance visual acuity by absorbing the light not captured by the photoreceptor cells, thus reducing glare. The most important task of the retinal pigment epithelium is to store and synthesize vitamin A, which is essential for the production of the visual pigment [3]. The pigment epithelium rests on Bruch's membrane, a basement membrane on the inner surface of the choroid.

There are two areas of the human retina that are structurally different from the remainder, namely, the fovea and the optic disc. The **fovea** is a small depression, about 1.5 mm across, at the center of the macula, the central region of the retina [11]. There, the inner layers are shifted aside, allowing light to pass unimpeded to the photoreceptors. Only tightly packed cones, and no rods, are present at the foveola, the center of the fovea. There are also more ganglion cells accumulated around the foveal region than elsewhere. The fovea is the region of maximum visual acuity.

The optic disc is situated about 3 mm (15° of visual angle) to the nasal side of the macula [11]. It contains no photoreceptors at all and hence is responsible for the blind spot in the field of vision. Both choroidal capillaries and the central retinal artery and vein supply the retina with blood. A typical fundus photo taken



Eye Features and Anatomy, Fig. 3 Fundus picture of a right human eye

with visible light of a healthy right human eye is illustrated in Fig. 3, showing the branches of the central artery and vein as they diverge from the center of the disc. The veins are larger and darker in appearance than the arteries. The temporal branches of the blood vessels arch toward and around the macula, seen as a darker area compared with the remainder of the fundus, whereas the nasal vessels course radially from the nerve head. Typically, the central **retinal blood vessels** divide into two superior and inferior branches, yielding four arterial and four venous branches that emerge from the optic disc. However, this pattern varies considerably [6]. So does the choroidal blood vessel pattern, forming a matting behind the retina, which becomes visible when observed with light in the near-infrared range [12]. The blood vessels of the choroid are even apparent in the foveal area, whereas retinal vessels rarely occur in this region.

In the 1930s, Simon and Goldstein noted that the blood vessel pattern is unique to every eye. They suggested using a photograph of the retinal blood vessel pattern as a new scientific method of identification [13]. The uniqueness of the pattern mainly comprises the number of major vessels and their branching characteristics. The size of the optic disc also varies across individuals. Because this unique pattern remains essentially unchanged throughout life, it can potentially be used for biometric identification [12, 14].

Related Entries

- ▸ Iris Device
- ▸ Retina Recognition

References

1. J. Pevsner, Leonardo da Vinci's contributions to neuroscience. Trends Neurosci. **25**, 217–220 (2002)
2. H. Davson, *The Eye*, vol. 1a, 3rd edn. (Academic, Orlando, 1984), pp. 1–64
3. A.J. Born, R.C. Tripathi, B.J. Tripathi, *Wolff's Anatomy of the Eye and Orbit*, 8th edn. (Chapman & Hall Medical, London, 1997), pp. 211–232, 308–334, 454–596
4. Ian Hickson's Description of the Eye, 1998 http://academia.hixie.ch/bath/eye/home.html
5. R. Warwick, P.L. Williams, *Gray's Anatomy*, 35th British edn. (W.B. Saunders, Philadelphia, 1973), pp. 1100–1122
6. C.W. Oyster, *The Human Eye: Structure and Function* (Sinauer Associates, Sunderland 1999), pp. 411–445, 708–732
7. L. Flom, A. Safir, Iris recognition system, US Patent No. 4,641,349, 1987
8. J. Daugman, Biometric personal identification system based on iris analysis, US Patent No. 5,291,560, 1994

9. J. Daugman, Iris recognition. Am. Sci. **89**, 326–333 (2001)
10. J. Daugman, Recognizing persons by their iris patterns, in *Biometrics: Personal Identification in Networked Society*, 2nd edn. (Springer, New York, 2005)
11. R.S. Snell, M.A. Lemp, *Clinical Anatomy of the Eye* (Blackwell Scientific, Boston, 1989), pp. 169–175
12. R.B. Hill, Fovea-centered eye fundus scanner, US Patent No. 4,620,318, 1986
13. C. Simon, I. Goldstein, A new scientific method of identification. N. Y. State J. Med. **35**, 901–906 (1935)
14. R.B. Hill, Apparatus and method for identifying individuals through their retinal vasculature patterns, US Patent No. 4,109,237, 1978