Issues and Advances in Biometrics

Sergey Tulyakov[a]and Venu Govindaraju[a],

[a]Center for Unified Biometrics and Sensors, University at Buffalo,
520 Lee Entrance, Suite 202, Amherst, NY 14228, USA

Biometrics is the automated recognition of the persons based on the structure of their body or their behavior. The expansion of the technology resulted in the availability of cheap and high performance biometric sensors, and made the functioning biometric systems a reality. In this chapter we briefly describe the main advances of biometrics research field. In particular, we will discuss the most widely used biometric modalities, fingerprint and face, present the main concepts of the measuring biometric system performance and combining biometric matchers. We will also devote our attention to some research directions further enhancing biometric systems: cancelable biometrics, liveness detection, indexing and individuality. The discussions are illustrated by the examples providing additional insight into this field.

1. Introduction

1.1. History of Biometrics

General descriptions of a particular person, including the height, color of the skin, hair and eyes, particular traits in appearance and behavior, have been possibly used since ancient times. Though such general descriptions might not be sufficient for person identification with complete confidence, they can be successfully used in constrained situations or for the confirmation of other, more discriminative, biometric features. These features are still widely used (e.g. on driver licenses) and might be called as *soft biometrics*. The fingerprints and face can be considered as the earliest traditional biometrics in use by people. Fingerprints have been known to be used by ancient potters to identify the produced goods [2]. Face portraits and sculptures might have been used for both identifying the important persons and marking goods. For example, coins bearing king head might serve both to confirm validity of the coin, as well as, help to recognize the king.

The biometric measurement began to play more increasing role with the increased amount of travel and bigger scale of industrial production in recent time. The modern use of biometrics has probably began with the development of Henry fingerprint classification system at the end of 19th century. In this system, each fingerprint of the person was checked on whether it had a whorl ridge structure. The total number of possible combinations of whorls for ten fingers is $2^{10} = 1024$; therefore, each person belongs to one of 1024 possible Henry fingerprint classification classes. The system was first employed at India to avoid the duplicate payments to factory workers. Later it was adopted by Scotland Yard to track criminals - after arresting a person the Henry classification system

was used to check whether this person already had a criminal record. At the same time, the techniques of lifting latent fingerprints at the crime scenes have been developed and increasingly used in forensics [2].

The wide use of face photographs and signatures in passports and other documents can be viewed as further expansion of biometric use in modern society. Until recently the process of biometric matching, e.g. between passport photo and person's face or between bank check signature and previously enrolled signature at the bank, relied on human experts. With the proliferation of computers we expect that computers would perform most biometric matching tasks. Also, with the development of new sensor technologies it becomes possible to employ a significant number of new biometric traits.

1.2. Modern Use of Biometrics

The purpose of biometrics is to provide a confident authentication of a person participating in some activity. Since the biometrics field is still young and the price of biometric systems is high, most of current biometric systems are deployed in high importance applications. Here is a sample list of some current biometric technology applications, clearly incomplete:

- *Access control*

  This is probably the most widely used application of biometrics. We can differentiate: 1. large scale applications, such as access to the country, 2. middle scale applications, such as access to work place, prison inmate control, hospital patient tracking, and 3. small scale applications, such as controlling access to computer or to the car.

- *Distribution of benefits*

  Just as in case of first use of Henry fingerprint classification system to avoid the duplicate payments to workers, biometrics is increasingly deployed for the purpose of controlling the distribution of social benefits. In contrast to access control applications the biometric system has to ensure that each person is not enrolled twice and, therefore, the benefits are not distributed twice to the same person. Pensions, salaries and medical insurance payments can benefit from biometrics use.

- *Financial transactions*

  If person's credit card is lost or stolen, a stranger would be able to use. Integrating biometrics with credit, debit and other types of payment cards can significantly reduce their misuse. It is not even necessary to have a card; a person might use a biometrics alone to identify himself to the financial system and authorize payments.

- *Forensics*

  Fingerprints had a long history of usage in forensics due to the property of human skin to leave them on touched surfaces. The development of FBI's AFIS (Automatic Fingerprint Identification System) showed the ability to automate the matching process and to perform a match of latent fingerprints to the database consisting of millions known fingerprints. DNA matching is another recently developed technique

used for the purpose of identifying criminals. The proliferation of biometric sensors, for example surveillance video cameras, will result in the collection of biometric data capturing suspects and in the possibility of such biometrics to be used in forensics.

With the further development of biometric technologies and the falling prices of biometric sensors and solutions we expect the biometric field to expand widely into modern life. Here are some possible future applications of biometric technologies:

- *Smart environments*

  The idea of smart environments is the increased interaction between the person and the surrounding environment enhanced with sensors and computing power. The biometrics might play an essential part in this interaction by recognizing who the person is and providing person-specific actions. For example, by recognizing who entered the room, the smart room might adjust the lighting and temperature according to that person's preferences. Or, the smart car might recognize the person sitting in the driver's seat and adjust rear-view mirrors accordingly.

- *Internet transactions*

  Current user-computer authentication is based on the remembering passwords; many websites require registration and entering authenticating passwords. Password authentication might be replaced by biometrics; instead of entering password a user might swipe a finger at fingerprint sensor and be authenticated. As another example, the smart video system might stream and show a rated movie only if built-in biometrics sensor recognizes that all people watching it are adults.

- *Total surveillance*

  The eventual development of sensor and biometrics technology might lead to the systems identifying and tracking all people at all times. It is hard to predict the consequences of such development, but it is clear it will have a significant impact on the society; one of the benefits frequently advertised is the elimination of crime. The deployment of city-wide surveillance system in London showed that significant progress in biometrics is still required in order for the system to work as expected.

1.3. The Structure of Biometric System

The typical biometric system consists of the following elements: biometric scanners located at the points where the person has to be authenticated, biometric matchers and the biometric database which stores the person's information and biometric templates. Depending on application the matchers and database can be located either at the dedicated server, at the location of the scanner, or be contained in the smart card belonging to the user. In all cases biometric system integrators have to ensure that no tampering has occurred to any of the system's elements or communication lines between them.

The work flow of biometric system has two operational stages - enrollment and authentication.

- *Enrollment*

The task of enrollment stage is to create a record about the person in the database together with biometric templates. Since the access to biometric database should be secure, the enrollment stage usually requires the presence of human operator. The operator should verify the identity of the user by alternative means and insert the enrollment record into biometric database. The successfully enrolled user is called *enrollee*. The protocol for enrollment might include the quality control of biometric templates and the check that this person is not already enrolled in the system or that there is no other enrollee with similar biometric templates (which will be the cause of errors during authentication stage). If some confusion exists, the user might be asked to re-scan the biometrics or to use additional biometric modalities. The biometric system might also update its indexing structure during enrollment.

- *Authentication*

The user is required to present the biometrics to the scanner, and biometric system matches input biometrics with the biometric templates stored in the database. The user might also be required to provide additional authentication information, e.g. some identification number, so that the biometric system would perform matching using only selected enrolled templates. The authentication stage might not need the presence of human operator; upon successful authentication the system might automatically authorize requested action.

1.4. Biometrics and Pattern Recognition

The research in biometrics uses many techniques of pattern recognition and thus can be considered as a part of this more general field. The processing of biometric input usually has all the traditional steps of generic pattern matching algorithm - preprocessing and enhancement, feature extraction and matching. Pattern recognition deals with classes and the number of the classes is rather small; some learning of the classes is frequently performed from training samples and the number of the training samples for each class can be large, hundreds or thousands. On the other hand, biometrics usually has only one enrolled sample template for each person (class), and class specific learning is rarely performed. The matching in biometric system can be viewed as simple nearest neighbor matching in traditional pattern recognition field; the input is classified as belonging to person with nearest enrolled template. From this point of view, the biometrics deals with rather simple subset of problems of pattern recognition.

On the other hand, the variation in the appearance of samples of the same class in biometrics can be significant, and sometimes bigger than the variation between samples belonging to different classes (see the examples of face images in section 2.2). Therefore, traditional pattern recognition methods oriented to the learning of class separation functions might not deal adequately with biometric problems. It becomes important in many biometric problems to learn a representational model - all possible ways in how person's biometric might appear on the scanner. The biometric matching in this case is transformed to matching models, rather than doing classification in the feature space.

2. Biometric Modalities

The structure of human body and person's behavior is rather uniquely determined by genetic and environmental factors. Some biometric characteristics, e.g. sex, skin and hair color, are determined by genetic make-up, some biometrics, such as fingerprint and iris, are formed during the fetus development, and other biometrics, such as voice and gait, are the product of the later life of the individual. Even if the face appearance of the person is mostly determined by the genes, the examples with monozygotic twins show that the environment can play a role in the face appearance in the later life.

It is not surprising, therefore, that practically any part of the human body or appearance can serve for the purpose of identifying individuals. The *biometric modality* is the choice of a particular body part or a particular person's behavioral characteristic for the purposes of biometric person authentication. Different biometric modalities usually require different sensors and matching algorithms. The adoption of a particular biometric modality is due to several factors: cost of the sensors, performance of the matching algorithm, convenience and acceptance by the users, universality of biometrics.

In the rest of this section we consider in detail most widely used biometric modalities: fingerprint, face and hand geometry. We will also shortly discuss the use of other modalities as well.

2.1. Fingerprint

The use of fingerprints for biometric purpose, especially in forensics, has a long history, and older databases were created using ink and paper. Recently, most fingerprint databases are collected using digital scanners directly, and older databases are digitized. The digitization of fingerprint scanning allowed using automatic algorithms for template extraction and matching. But, digital fingerprint templates produced by different types of scanners vary significantly in their appearance. Figure 1 presents sample fingerprint images from three fingerprint scanners taken from FVC 2002 database [20].

Most fingerprint matching algorithms rely on the extraction and matching special points of the fingerprint ridge structures - *minutia*. Usually minutia points designate ridge endings and ridge bifurcations, and have a representation (x, y, θ), where x and y are coordinates of the minutia in the image and θ is the direction of minutia coinciding with the orientation of ridges at these coordinates. In order to extract minutia, the following steps can be followed:

- Find the orientation and strength of ridges in in each point (or small blocks) of the image. This can be achieved by different methods, for example by using wavelet or Fourier coefficients, or by directly analyzing image gradients. The important properties utilized here is the wavy nature of fingerprint ridges; the ridge directions change gradually, the image gradients (directions of fastest change in image intensity) are perpendicular to ridge directions, and wave structure makes the use of wavelets or Fourier coefficients natural. Thus, even if different sensors produce quite different fingerprint appearances, the orientation and general ridge structure can be relatively easy be found.

- Enhance and binarize image. Using the found direction and frequency of the ridges in each point of the fingerprint, a filter, e.g. in wavelet or Fourier domain, can be

(a) DB1 (b) DB2 (c) DB3

Figure 1. Samples of fingerprint images from Fingerprint Verification Competition (FVC), 2002. Included images from databases DB1, DB2, DB3 were obtained using different fingerprint sensors.

applied emphasizing the ridge direction and frequency and removing other directions and frequencies as noise. Consequently, a simple threshold can be used to binarize the image.

- Segment the fingerprint area from the background. This might be considered as the most difficult part of fingerprint image processing. Whereas some thresholding techniques might be successful on fingerprints with white background (DB1 image in Figure 1), they will not be sufficient for sensors producing complex background. Additional problem is the frequent presence of residual fingerprints - the latent fingerprints formed on the surface of the scanner by the previous users. Usually, some heuristics, for example involving the strength of ridges, the confidence in the extracted ridge directions and frequencies, can be used for segmentation.

- Extract minutia positions. Different techniques can be used here - thin the binary image to obtain 1 pixel wide skeleton and find its endpoints and bifurcations, find the contour of the binary image and extract minutia points as the points of large change in direction of the contour, or follow the ridges with perpendicular cuts and find where these cuts end or merge.

Note, that presented steps are not necessary and many other techniques have been investigated [20], for example, it is possible to extract minutia positions directly from the gray-scale image. We present an example of binarized fingerprint image and the candidate locations of minutia positions in Figure 2; the image was enhanced and binarized using filtering of Fourier coefficients in 16x16 pixel blocks of the image, and the candidate minutia positions were found by following contours of binary image [5].

The set of extracted minutia usually represents a fingerprint template stored in the database, but the template might also contain other elements useful for fingerprint match-

Figure 2. Binarized fingerprint with candidate minutia positions.

(a) 1_1.tif (b) 1_2.tif

Figure 3. Two matched fingerprints with marked matched minutia positions.

ing, e.g. ridge orientation map, counts of ridges between minutiae, original gray-scale fingerprint image. The type of the fingerprint, e.g. whorl as in Henry's system, can also be automatically extracted and used for matching or indexing.

The task of minutia matching algorithm is to find correspondences between two sets of minutia. It is usually assumed that the map responsible for minutia correspondences is affine (composed of rotation and translation). The brute force approach to minutia matching will look at all pairs of minutia in two fingerprints and assume that these minutia correspond to each other (pivot minutia); this assumption automatically determines the translation from minutia coordinates and rotation from minutia directions, and all other minutia are checked for correspondence with found transformation parameters. The brute force algorithm is somewhat slow, and many improvements can be made to it. For example, we might want to consider pivot minutia only if these minutia have similar neighborhood structure determined by the minutia and its two nearest neighboring minutia. The features extracted from minutia triplets are called *secondary features* in [16] and can be used instead of original minutia for more precise and faster matching. The set of matching minutia in two fingerprints obtained by the method of matching secondary features is shown in Figure 3. The final matching score is usually some heuristic function including number of matched minutia, numbers of minutia in two considered fingerprints and other parameters.

2.2. Face

The face biometrics can be considered as most convenient and universally acceptable biometric modality. The number of digital cameras, including webcams and cellular phone cameras, is significantly more than the number of fingerprint (or any other biometric) scanners. Therefore, there is a big incentive to utilize this multitude of cameras for biometric purposes.

The earliest works on face recognition relied on specialized algorithms to extract the

positions of *landmark points*, such as eyes, eyebrows, nose, mouth, and on measuring the distances between these points. The explicit extraction of landmark points follows traditional pattern recognition approaches of feature extractions, and performing classifications using feature vectors. Though such matching methods have good sense, it turns out that, due to large variations in the appearance of landmark points, it is rather difficult to confidently extract their positions. Subsequently, the implicit extraction of feature vectors by projection methods proved to have better performance and became the most popular face matching approach.

The work of Turk and Pentland [30] introduced a technique called *principal component analysis* (PCA) which had a major influence on the development of the face recognition research. Face images can be represented as points in $W \times H$-dimensional space (W and H are the widths and heights of the image in pixels). Points corresponding to faces can not occupy the whole space since there are images representing other objects. The PCA technique attempts to approximate the region with faces by the linear subspace. Using the criteria that the sum of squared distances from the subspace to sample face images should be minimized, the optimal subspace is the subspace spanned by the first K eigenvectors of covariance matrix constructed using sample face images (K is the desired dimension of subspace; usually it is taken as the one which gives best recognition results). *PCA projection* is the orthogonal projection of original face images onto found from training samples *PCA subspace*, which is spanned by *principal components* - first K eigenvectors or *eigenfaces*. The example of PCA technique is shown in Figure 4. Each face-like image is a principal component projected back into image space (eigenface); a real face of person can be approximated by the linear sum of these principal components.

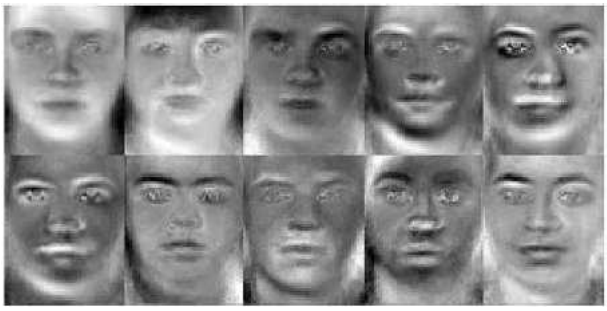


Figure 4. Sample eigenfaces of PCA model (images provided by R. Rodriguez).

The PCA technique can be used for two different purposes. First, by calculating the distance from the test image to the PCA subspace we can judge whether the test image represents a person's face or some other object. Many *face detection* techniques successfully use PCA. Second, two PCA projections of two different face images are K-

dimensional vectors of *PCA coefficients*, and the distance between these two vectors can serve as matching measure between two face images. The PCA and similarly constructed linear (some non-linear methods are also been investigated) projection algorithms [12] make the largest share of face matching methods.

Though projection techniques are able to get satisfactory matching results on some databases containing frontal and uniformly illuminated face images, their performance decreases significantly when any of the typical face variations appear: change in illumination, head rotation, occlusions, facial expressions and speaking dynamics. Figure 5 shows the examples of face images from CMU PIE (Pose, Illumination and Expression) database [25]. It is clear, that by using eigenfaces of Figure 4 it will not be possible to properly represent these faces and have a matching algorithm.

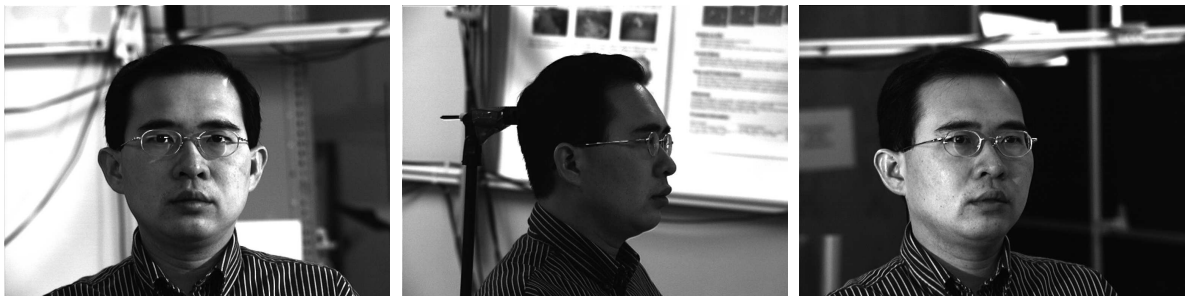


Figure 5. Samples of face images from CMU PIE [25] database. The great variation in the face position and illumination makes most projection-based matching methods and algorithms relying on feature extraction from landmark points ineffective.

We can view the PCA algorithm from two sides: on one side it is a projection of original image onto lower-dimensional feature space, and on the other side it is representation or the model of the face by K latent variables (same as feature vector). The PCA model of the face is quite simple - the face is a linear combination of eigenfaces and the coefficients in this combination are the latent variables. It is possible to construct more complex face models which more adequately represent the face and face variations.

Active Appearance Model (AAM) [8] was successfully utilized for face modeling. In this model, instead of using projections of whole face, the principal component projections for small patches around face landmark points are constructed (*texture PCA*). The set of distances between landmark points is also represented by the PCA projection (*shape PCA*). The model is matched to the face image by searching the best position of landmark points. For a particular choice of landmark points the match confidence is a sum of matching confidences from texture and shape PCAs. Active appearance models show good performance and are increasingly utilized in many tasks: face detection, face recognition, facial expression analysis. But active appearance models might still not work well with changes in illumination and head rotation, and special adjustments to the algorithm are needed [1].

3D morphable model [3] gives an example of even more complex face model. Instead

of a set of landmark points in two-dimensional plane for AAM, the surface in three-dimensional space is used to represent the shape of the face. The shape model is learned from a set of separately obtained 3D face scans by constructing PCA model. In addition to shape model, a texture model is constructed from the appearance of each pixel of the shape model - pixel color values. Again, the PCA model is used to represent textures.

Note, that though the 3D morphable model algorithm represents a face as surface in a 3-dimensional space, it is used to match 2-dimensional images only. The important part of the algorithm is to construct a model from a given the face image. During this construction the rotation of the head and the position of illumination source are estimated, as well as, shape and texture parameters of the model. Thus, this algorithm is inherently designed to deal with head rotations and changes in illumination, and it shows superior performance on the images from CMU PIE database of Figure 5.

2.3. Hand Geometry

Different biometric modalities exhibit different levels of variation; as a consequence the matching algorithms have different complexities. We might think that face matching requires rather complex algorithms (if we want to deal with head rotations and illumination changes) and fingerprint matching has rather medium complexity. Here we consider an easier biometric modality - hand geometry.

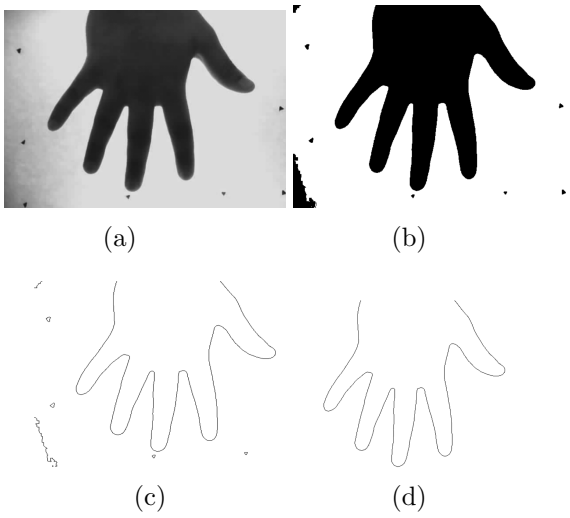


Figure 6. Different stages of processing hand image.

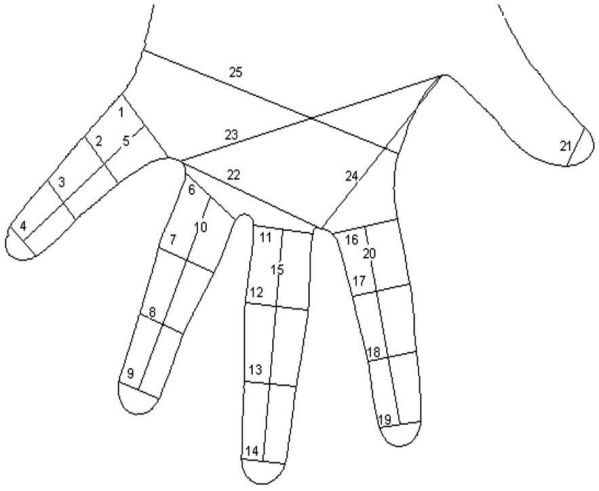


Figure 7. The features utilized for hand geometry matching.

We describe an algorithm for hand geometry matching used in [21]. Though there are specialized hand geometry scanners (e.g. including pegs for precise positioning of the hand and using laser for scanning), the hand images can be easily obtained with regular digital camera (Figure 6a). Simple binarization is applied in Figure 6b and the boundary

contours are extracted in Figure 6c. Using some heuristics, all the contours except one corresponding to the hand are discarded in Figure 6d.

The set of predefined features is extracted by searching the particular points of the hand contour - extrema where either the direction or the convexity of contour changes, Figure7. The features are usually the distances between these points, or some functions of distances (e.g. ratio of distances). The euclidean distance between feature vectors serves as (inverse) confidence of biometric match.

2.4. Other Modalities

It would be impossible to describe all investigated biometric modalities in this short chapter. In this section we only mention the most popular ones.

The *iris* is colorful ring-like structure around the pupil of human's eye. The iris turned out to provide good properties for person identification: diversity, small intrapersonal and large interpersonal variations, protection from the outer environment and little change with the passage of time. The binary vector of length 2048 is extracted by quantizing the responses of Gabor wavelets at the circular grid locations throughout the iris in [10]. The match distance between two irises is calculated as the Hamming distance between two binary feature vectors. Due to small variation in the irises of the same person and the relative ease of locating irises in images we might consider iris biometrics as a simple to implement. The most difficulty might be due to making good scans of irises, especially at a larger distances.

Speaker identification was one of the first automatic biometric applications investigated. The main advantage of speech modality is the abundance and cheapness of sensors - microphones. But, despite a significant research effort, speaker identification systems have shown only average performance. The performance of speaker identification systems is degraded in the presence of noise, and thus they are not suitable for many applications. Additional drawbacks of speaker biometrics is the inconvenience to the users (the necessity to actively speak) and high non-universality. But, so far, it is the only biometrics allowing remote authentication by means of phones, and this is how it mostly used.

Handwritten signature has been used for a long time to identify the documents to belong to particular persons, and similarly it can be used for the person identification. Some research into automatic matching of handwritten signatures has been performed, but the reported performance is not very strong. The *online handwritten signature*, providing time of writing in addition to position, has substantially better performance than *offline handwritten signature*. Though it can be used for the current widespread application of signature verification during credit card transaction, it is not clear if it would be more cost effective than replacement of signature by other, more convenient, biometrics, such as fingerprint or face.

Some newly developed biometric modalities rely on specific biometric sensors. *3-dimensional face* (or rather head) uses special sensor (e.g. laser) to obtain a 3-dimensional structure of person's head. *Blood vessel* biometrics might need a camera operating in infrared, and not in traditional visible light, spectrum. *Retina* biometrics uses blood vessels located inside person eyes; though it has good properties of performance and the preservation of features, many users might object to the intrusiveness of the retina scans. *Gait* biometrics might be useful in surveillance applications, where the distance to the subject

is typically large and most of the other biometrics fail to acquire usable templates.

3. Evaluating Performance of Biometric Systems

The important question facing biometric system designers is the evaluation of performance. We want to be able to say that one biometric matcher will perform better than the other, and, in general, that using a biometrics system is beneficial for the current application. It turns out that the evaluation depends on a particular application - one biometric matcher might have better performance than the other in one application, but worse performance in another application. In this section we present some ways to evaluate the performance of biometric matchers.

3.1. Operating Modes of Biometric Systems

The biometric system in a particular application is usually utilized in one of the following modes of operation:

- *Verification*

  In order to be authenticated the user first claims his identity, e.g. by presenting an I.D. card or by simply entering his name or identification number on the keypad. Then the user's biometric is scanned and matched against a single template corresponding to the claimed enrolled identity. The decision to accept the identity claim or reject it is usually made by comparing a single matching score to the threshold.

- *Identification*

  No claim of identity is made by the user, and the user's biometric is matched against all enrolled persons. *Closed set identification* systems assume that the user is always enrolled in the system; the identification is successful if the score corresponding to the true user's identity is better than all other matching scores. *Open set identification* systems assume that user might not be enrolled in the database and in such cases the correct decision of the identification system will be to reject identification attempt. Thus, in such systems, not only a best matching score is found, but it is also compared to some threshold.

- *Watch list or Screening*

  Watch list is the biometric application reverse of open set identification system. The input biometrics is matched against all persons in the database and the decision is made on whether the person is enrolled or not. In contrast to open set identification, we might not need to know which enrollee matches current user.

All modes of operation deal with two types of scores - *genuine matching scores* are the result of matching biometric templates of the same person, and *impostor matching scores* are the result of matching biometric templates of the different persons. The task of verification system is to determine whether a particular score is genuine or impostor, the task of identification system is to make sure that genuine score is higher than any impostor score and the task of watch list is to make sure that all scores produced during matching are impostors. Different tasks assume that the cost of errors made by a biometric

system is calculated differently. Therefore, some biometric systems might be suited for one operating mode, and some might be better suited for other. The example of section 3.3 shows that changing costs for system errors in verification system might change the choice of biometric matcher.

3.2. Performance of Verification Systems

The biometric system operating in verification mode makes a decision on whether the score is genuine and has two possible types of errors: *false accepts* (FA), where an impostor score was accepted, and *false rejects* (FR), where a genuine score was rejected. False accept rate, FAR, is the proportion of accepted impostors among all impostors, and false reject rate, FRR, is the proportion of rejected genuines among all genuines. The decision usually consists in comparing the score to the threshold, θ, and both error rates are functions of θ: $FAR(\theta)$ and $FRR(\theta)$.

Suppose we know what are the densities of the scores: $p_{gen}(s)$, the density of the genuine scores, and $p_{imp}(s)$, the density of the impostor scores. Then, the $FAR(\theta)$ and $FRR(\theta)$ can be expressed as (assuming accept decision if score is bigger than θ):

$$FAR(\theta) = \int_{s \geq \theta} p_{imp}(s)ds \quad , \quad FRR(\theta) = \int_{s < \theta} p_{gen}(s)ds \tag{1}$$

If we obtain a sample of genuine and a sample of the impostors scores of a biometric matcher, we can approximate $p_{gen}(s)$ and $p_{imp}(s)$, e.g. by using mixture of gaussians or Parzen window method. Though it might be possible to calculate $FAR(\theta)$ and $FRR(\theta)$ using approximated densities and equations 1, it would be easier to simply count the proportion of sample impostors above threshold and the proportion of sample genuines below threshold. Figure 8 shows the densities of genuine and impostor scores of face matcher 'C' from NIST biometric score set BSSR1 approximated by Parzen window method. The integrals of equations 1 are represented as the areas under corresponding densities; threshold $\theta = 0.4$ was used for acceptance decision.

The graphs of score densities of Figure 8 might be helpful to visualize the distributions of scores in a biometric system, but they are of little use for making comparisons of biometric systems. Since both FAR and FRR depend on the single parameter, it is possible construct a graph $\{FAR(\theta), FRR(\theta)\}$ representing a trade-off between two types of error depending on threshold parameter θ. Such curve is called *ROC curve* (ROC stands for Receiver Operating Characteristic). Note, that this curve might also be called DET curve (Detection-Error Trade-off), and FRR axis can be changed to GAR (genuine acceptance rate) axis.

The ROC curves for face matcher 'C' and for fingerprint matcher 'ri' (to be precise, 'ri' stands for 'right index' match scores of fingerprint matcher 'V') from NIST BSSR1 database are shown in Figure 9. The closer ROC curve to the axes, the less errors biometric matcher has, and consequently, has better performance. As ROC curves for both matchers show, there might not be a short yes/no answer that one matcher is always better than another matcher. If our preference is to have lower FAR, for example in a high-security application requiring fewer false accepts, then we need to use matcher 'ri'. If we need more convenience to the users and smaller number of false rejects, we need to use matcher 'C'. Sometimes, the *Equal Error Rate* (EER) is used for comparison, which is defined as the point in ROC curve where $FAR = FRR$ (shown in the figure); in this

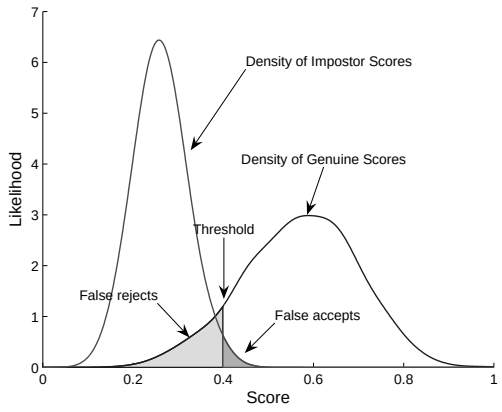


Figure 8. The densities of genuine and impostor scores of face matcher 'C' (linearly normalized to $[0, 1]$). The areas corresponding to the rates of false accept and false reject errors for threshold .4 are shown.

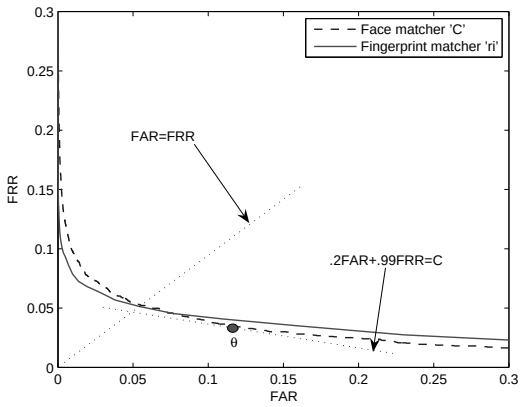


Figure 9. ROC curves for face matcher 'C' and fingerprint matcher 'ri'. 'C' has better performance for low FRR values, and 'ri' has better performance for low FAR values.

case $EER = FAR = FRR$. In the next section we present a practical example on how the biometric systems can be evaluated with respect to a particular application.

3.3. Example

Consider the application of biometrics to control the access to an amusement park. The user enrolls into the system during the first visit to the park, when her biometrics is scanned and stored in the database. On subsequent visits the scanned biometric input is matched against the stored template (retrieved with the help of entrance ticket identification number). If match decision is made by the biometric system, the user is let in, and if no match is declared, the user is asked to re-scan biometrics and/or human supervisor is called to verify the identity of the user by alternative means (e.g. driver's license).

In order to optimally choose the biometric system for this application, we might want to consider the following cost function:

$$Cost = C_{FA} P_{imp} FAR(\theta) + C_{FR} P_{gen} FRR(\theta) \tag{2}$$

where C_{FA} is the cost associated with making erroneous accept decision, C_{FR} is the cost of making erroneous rejection, P_{imp} and P_{gen} are the prior probabilities of impostor and genuine matches (impostor or genuine user attempting to get access), $FAR(\theta)$ and $FRR(\theta)$ are error rates of considered biometric system. The costs of making decision errors and prior probabilities should be estimated by the park administration. For example, the cost of making erroneous accept decision, C_{FA}, is the cost of servicing user in a park, say \$20; the cost of erroneous reject (time spent by servicing personnel, dissatisfaction of the user and reduced possibility of making repeated ticket sale to this user, dissatisfaction of other users waiting in line) might be estimated as \$1; the probability of impostors (users with

stolen, borrowed or fake ticket trying to get unauthorized access to the park) might be estimated as 1% and the probability of genuines is correspondingly 99%. In this case, the total cost of making biometric decision error is

$$Cost = 20 * .01 * FAR(\theta) + 1 * .99 * FRR(\theta) = .20FAR(\theta) + .99 * FRR(\theta) \quad (3)$$

Suppose, as in Figure 9 we are evaluating two matchers with regards to this cost equation. The lowest overall cost will be achieved by finding the intersection of line $.2FAR + .99FRR = C$ with any of the ROC curves. Such intersection is denoted in Figure 9 as θ and face matcher 'C' achieves lowest cost. Note, that if we had different estimates on costs of errors or prior probabilities of each type of users, we might have gotten different biometrics preference. For example, if we had $P_{imp} = 10\%$ of impostors trying to gain unauthorized access to the park, our cost would have been $Cost = 2FAR + .9FRR$ and fingerprint matcher 'ri' would have achieved lower cost.

In order to decide whether the deployment of biometric system would be beneficial, we need to account for more factors. The total cost would be the sum of cost given by equation 2, the cost of purchasing and maintaining biometric system and the implicit cost of inconvenience to the visitors of the park. The additional revenue will be due to reduced number of unauthorized users getting access to the park, consequent increased number of ticket sales and less dissatisfaction of legitimate users from sharing the park facilities with unauthorized users.

4. Multimodal Biometrics

Multimodal biometric system uses more than one biometric modality for the authentication of the user. There are two major advantages for using such systems:

1. Properly constructed combined system will have better performance than the system using only a single biometric modality.

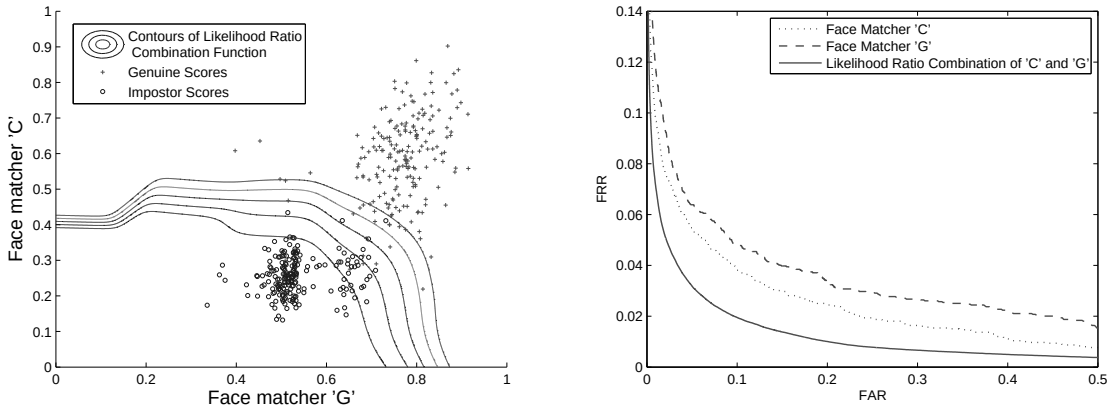
2. It is more difficult for an intruder to bypass the security of multimodal system since more modalities need to be faked.

The possible drawback of multimodal systems is the need for additional biometric scanners and more time needed for the user to be authenticated. The drawback might be reduced if scanners of different modalities can be combined in one device. For example, it is possible to have a combined scanner for face and for iris utilizing one or two digital cameras with different resolutions in one unit. Or, fingerprint scanner can be combined with finger blood vessel scanner; in this approach the blood vessel scanner can use similarly positioned camera which is more sensitive to infrared spectrum of light than the camera for the fingerprint ridges.

4.1. Combination in Verification Systems

Without loss of generality, assume that we have two scanners for different modalities or two matching algorithms using the input of one scanner (instead of arbitrary many scanners or matchers). Both matchers deliver two matching scores, s_1 and s_2, and our task is somehow combine them in a single matching score, $S = f(s_1, s_2)$, so that the performance of combined matching system was optimal. The problem of finding the

combination function f is quite simple for the biometric systems operating in verification mode.



(a) (b)

Figure 10. Likelihood ratio combination of face matchers 'C' and 'G' from NIST BSSR1 biometric score set: a. Few samples of genuine and impostor score pairs from both matchers and the contours of likelihood ratio combination function (scores in both matchers are linearly normalized to interval $[0, 1]$. b. ROC curves of standalone matchers and their combination by likelihood ratio function.

Let score pairs (s_1, s_2) be the points in the two-dimensional space in Figure 10(a). This space can be regarded as the feature space for a classification algorithm trying to separate two types of points - points corresponding to either genuine or impostor score pairs (s_1, s_2). The performance criteria of verification systems, minimizing the trade-off between two types of errors, false accepts and false rejects, directly corresponds to the criteria of minimizing misclassification cost of our two-class classification problem. The solution to such problem is well-known in pattern classification field: the optimal decision function f can be taken as the likelihood ratio of two classes:

$$f(s_1, s_2) = \frac{p_{gen}(s_1, s_2)}{p_{imp}(s_1, s_2)} \tag{4}$$

The densities of score pairs $p_{gen}(s_1, s_2)$ and $p_{imp}(s_1, s_2)$ can be approximated by different methods using a *training set* of sample score pairs. Alternatively, a classification can be performed by many developed methods of pattern classification field without explicit approximation of score densities. Generally, many pattern classification algorithms can deliver better approximation of decision boundaries than the explicit use of approximated densities in likelihood ratio method, but the difference is not significant. Since the dimension of feature vectors in classification problem coincides with the number of matchers and this number is usually small, the densities approximation methods will have adequate

performance. Figure 10(a) shows the decision boundaries (contours $f(s_1, s_2) = \theta$) of likelihood ratio combination method for combining face matchers 'C' and 'G' of NIST BSSR1 dataset, as well as few samples of genuine and impostor score pairs. The two dimensional densities were approximated using Parzen window method. Figure 10(b) contains ROC curves of single matchers and of their combination using likelihood ratio.

4.2. Combination Rules

One of the research directions in classifier combination field investigates the use of so called combination rules [18]. The combination rules specify that the matching scores should be combined in some predetermined fashion, for example, sum rule adds scores $f(s_1, s_2) = s_1 + s_2$ and product rules multiplies them $f(s_1, s_2) = s_1 \times s_2$. Usually, some assumptions are made on the nature of scores, and one or the other rule is justified.

If the matching scores were truly satisfying some required assumptions, the use of particular combination rule might have made sense. In practice, the matching scores are the result of elaborate calculation of distances between two biometric templates, and there is no reason to expect that some assumptions on these scores, e.g. scores are approximations of posterior class probabilities, hold. We might try to convert the matching scores to satisfy required condition, but such conversion would require some learning algorithm using a training set of scores. In this case the task will be somewhat equivalent to learning combination function. Learning combination function directly seems to be an easier approach to combination.

One of the reasons used to justify combination rules is the existence of independence between scores produced by matchers of different modalities. The independence knowledge might be easily exploited for likelihood ratio combination method: instead of approximating two-dimensional score densities $p_{gen}(s_1, s_2)$ and $p_{imp}(s_1, s_2)$, we can decompose them in one dimensional components

$$p_{gen}(s_1, s_2) = p_{1,gen}(s_1)p_{2,gen}(s_2) \quad , \quad p_{imp}(s_1, s_2) = p_{1,imp}(s_1)p_{2,imp}(s_2) \tag{5}$$

and approximate one-dimensional components. As our research shows [27], such decomposition and approximation of one-dimensional components indeed improves the performance of combination algorithm, but the gains are very small.

4.3. Combination in Identification Systems

There is almost no research investigating the combination of biometric matchers in identification systems. Usually it is implied that the same combination function f which was constructed for verification system can be similarly used for combinations in identification systems. The likelihood ratio combination function of equation 4 seems to be a good candidate for the combinations in identification systems.

As we investigated in [28], the likelihood ratio combination function might not deliver the optimal performance for identification systems. It is actually possible, that the combination in identification system using likelihood ratio function will have worse performance than a single matcher used in combination. The optimal combination function for identification systems might not have convenient analytic representation as likelihood ratio function, and finding it is an open research question. We have proposed some combination methods [29] that work better than likelihood ratio in identification systems, but the optimality of these methods is uncertain.

4.4. Increase in Performance

Is performance of combined system always better than the performance of any single matchers used in combination? It is clear that in worst case, we can always have a combination function to simply output a score of single matcher, e.g. $f(s_1, s_2) = s_1$, and therefore the performance of optimal combination algorithm can not be worse than the performance of a single matcher. But, the increase in performance is not guaranteed when the number of matchers is increased. If, for example, two matchers operate on the same modality, they might have very similar matching results, and combining them will have little effect. It is usually hypothesized that the increase in performance is largest when combined matchers produce statistically independent matching scores, but no published evidence for such hypothesis seems to exist.

5. Additional Topics in Biometrics

5.1. Cancelable Biometrics

If a traditional security system utilizing passwords is compromised, and the intruder gains access to the passwords, the old passwords can be easily revoked and new passwords issued. If we want to utilize biometrics in the analogous system, we need to ensure that enrolled biometric templates could be revoked and new biometric templates are issued; the intruder possessing compromised biometric templates should not be able to use them. The biometrics implementing this capability is called *cancelable biometrics*.

There are two obstacles for constructing cancelable biometric templates. The first obstacle is the permanent nature of biometrics - it is not possible for the users to change their biometrics as they could do with the passwords. In order to overcome this obstacle any cancelable biometric system should combine the permanent biometric features with some replaceable key in order to create cancelable templates. The second obstacle is the variation of biometric measurements and the necessity to match close but non-identical scanned biometrics. If we are dealing with traditional passwords, one-way hash function (such as MD5) can be applied, and only password hashes could be stored; the password match would succeed only if identical password is entered and its hash exactly coincides with the stored hash. Since the biometric measurements of the same person are not identical, this method can not be applied directly to the biometric templates.

One idea to deal with the variability of biometric templates is to utilize error correcting codes. Error correcting codes are mostly used in the transmission of digital data. If the part of the data is corrupted, the error correction algorithm might be able to recover the original data. Suppose, b is the binary representation of the biometric template and let c denote the error correction bits, such that the concatenation $b||c$ represents a valid codeword of the used error correction system. If b' is another sample of the same person's biometric and the difference between b and b' is sufficiently small for chosen error correction system, then $b'||c$ can be corrected to $b||c$. Such application of error correcting codes allows us to eliminate storing biometric template b in the biometric database: instead of b, we store error correcting bits c and some hash of the string b: $h(b)$. During authentication user presents biometrics b' and using stored c the original b is calculated; the hash of restored template is compared to stored hash $h(b)$ and, if they are identical, the match is declared. Note, that if intruder obtains stored values of c and $h(b)$, he would not be able

to restore b.

The above algorithm for hiding biometric data has been presented in [11]. The biometric b can be combined with replaceable key k, b_k, before calculating c and $h(b_k)$ in order to make the biometric cancelable, but it is not clear if this enhancement is really needed. Indeed, if we assume that intruder is smart enough to reverse (generally non-reversible) hash function and obtain b_k from the $h(b_k)$, then it is probable that he would be able to obtain k and reverse b_k to get b as well.

Although described algorithm can be applied to many biometric modalities whose templates are represented by a slightly varying binary string b, there are biometric modalities which do not have such representation. For example, the fingerprint templates usually contain a set of minutia, whose quantity, order and values can change significantly. Most of the recent research in cancelable biometrics deals specifically with fingerprint templates represented as a set of minutia. Juels and Sudan [17] proposed a construction of *fuzzy vault*, which allows comparison of two non-ordered sets of features, and Clancy et al. [6] applied fuzzy vaults for storing fingerprint templates. Most of the subsequent research into fingerprint fuzzy vaults deals with their two major weaknesses - the corresponding minutia positions of two compared fingerprints should be exactly the same, so the fingerprints should be pre-aligned before fuzzy vault construction, and the requirement of using unprotected fingerprint during matching to fingerprint stored in fuzzy vault (intruder can simply intercept these unprotected fingerprints instead of trying to break the fuzzy vault). The more detailed analysis of the security weaknesses of fingerprint fuzzy vaults and other cancelable biometrics is presented in [24].

There are also proposals of hiding fingerprint templates not involving the error correcting codes. For example, in [13] and [26] authors construct hashes of fingerprint minutia sets so that the matching of two fingerprints is performed by using only their hashes. No fingerprint pre-alignment is needed, and hashes can be constructed securely at the scanner location so that original templates are never transmitted or stored. Though such approaches are sometimes criticized for the degradation of matching performance, such degradation should be expected. As we explain in section 5.5, the combined use of biometrics and user specific keys can result in apparent perfect performance of biometric systems, but such results are misleading. Therefore, the algorithms constructing cancelable biometrics and claiming performance superior to the original non-cancelable biometrics should be considered with caution.

5.2. Liveness

Even if an intruder gets access to unprotected templates stored in the biometric database, these templates might be of no use if the biometric system implements some kind of liveness test during biometrics acquisition. For example, by presenting a face photo to a camera, the intruder might trick the face biometric system to perform a match of the photo instead of live face. If the stored biometric templates use some features and not original images of faces, it is usually easy to construct an artificial face image having same features as a particular biometric template and use such image for breaking the system. By implementing additional liveness test, the biometric system can avoid such break-ins.

The particular technique for liveness detection would greatly depend on biometric modality. For some modalities, such as face and speech, we can use an *active liveness de-*

tection working on a challenge-and-response principle - during the biometrics acquisition the user might be asked to turn head, smile or speak a particular sentence. For other biometrics, e.g. fingerprint, such method will not work and we need to devise a *passive liveness detection*, which searches for the specific properties of live biometric scans. For example, the fingerprints produced by the synthetic gummy finger might have smoother edges than fingerprints of the live fingers, as well as have no sweat pores. The fingerprint image processing algorithm might look for these specific features and determine if the used finger was artificial.

Sometimes the liveness detection might require the use of separate scanner. For example, the determined intruder might simply cut off the finger of person in order to bypass a security system. The scanned fingerprint in this case will be practically the same as coming from a live fingerprint if traditional fingerprint sensors are used. But, if the fingerprint scanner also incorporates the sensor able to analyze the chemical blood content, the liveness of the fingerprint can be easily detected.

5.3. Indexing Biometric Databases

As we already pointed out in section 3.1, in addition to more widespread verification mode of operation, the biometric system can operate in other modes, for example, identification and watch list modes. These other modes might require the matching of input biometric templates to a set of N biometric templates enrolled in the database. But the biometric matching usually takes a significant time. For example, matching two fingerprint or two face templates can typically take up to one second. If the database contains a large number N of enrolled persons, e.g. millions, matching input template to all enrolled templates will require a prohibitively large time. Therefore, in order to deal with large-scale biometric applications, some kind of indexing algorithm should be used in the system.

If the biometric templates are represented as fixed length feature vectors, then traditional indexing techniques in multidimensional space, such as kd-trees, can serve as a basis for biometric index. For example, in [21] a pyramid technique was used to index hand geometry biometrics. Such techniques are most helpful when the dimension of feature vectors is rather small. If the dimension of the feature vectors is large, for example $\tilde{1}000$, multidimensional indexing techniques might not be effective. But, the ordered nature of biometric templates makes the distance calculation between them relatively fast and still allows their use in large-scale real-time applications. For example, an iris recognition system deployed in the watch list mode [9] is able to perform a significant number of matches, since each match consists in a fast calculation of Hamming distance between two binary iris templates.

The situation is more difficult when the biometric templates do not have fixed length feature vector presentation. Fingerprint templates usually consist of a minutia set of a variable size and with no particular order. Moreover, the coordinates of corresponding minutia in two fingerprints can differ significantly due to their translation and rotation. Therefore, the simple, euclidean-like, calculation of distance between two templates is not possible. Hence, above described techniques are not applicable - we are not able to perform multidimensional indexing, and we are not able to simply match every template in the database.

The construction of fingerprint indexing algorithm turned out to be a rather difficult task. Three general approaches for reducing match time exist. The first approach is to classify all fingerprints into few classes (usually five) of the Henry classification system, and perform matching of the input fingerprint only to enrolled fingerprints of the same class. Many algorithms for doing such classification were proposed, but the existence of only few classes is an inherent limiting factor for this approach. The second approach relies on representing fingerprint as a fixed length feature vector. The features are usually extracted from the orientation field of fingerprint ridges, and finding common frame of reference (for example, core positions) might be required [4]. The third approach tries to use minutia triplets to construct position invariant fingerprint representation, fingerprints are matched based on the number of similar triplets and the transformations between these triplets [15]. The input fingerprint is still practically matched against each enrolled template, but, in contrast to second approach, does not require separate processing of orientation fields and finding reference frame. The last two approaches have better performance than first approach based on Henry classification, but still not sufficient for large scale deployment (retrieving 10% of enrolled templates has 90% probability of getting correct match).

5.4. Individuality of Biometrics

Is it possible for two different persons to have almost identical fingerprints or face appearances? The research into *biometric individuality* tries to investigate this question. It is clear, that biometric measurements of the same person are not absolutely identical and some variation always exists. It would be interesting to know the chances of an impostor template to be within the boundaries of this variation. The individuality research has most impact on the forensic investigations. It also defines the best possible performance of biometric systems and separate biometric modalities.

Since the introduction of fingerprints in the criminal investigation, it was important for the prosecution to prove that the latent fingerprints found on the crime scene match exactly the fingerprints of the suspect, and do not match fingerprints of any other person. The first known individuality model of Galton [14] randomly placed minutia on a grid and calculated the probability that specific grid locations are chosen. Most subsequent models used similar designs and reported almost negligible probabilities that two fingerprints of different persons would match. As a consequence, the fingerprint evidence was considered as infallible in the courts for a long time.

But, the time showed that few errors in the fingerprint matching did happen [7]. The errors have become more visible when the DNA evidence took more central role; some fingerprint matching evidence have been overturned by the DNA evidence. The most important case occurred in 2004, when the innocent person has been arrested as a suspect of Madrid terrorist bombing [7]. The degree of the incorrect fingerprint match was exceptionally high - around 15 minutia were matched in two fingerprints, as well as, some third level features - sweat pores (12 matching minutia are sometimes regarded as sufficient for the positive match by FBI). The errors might also be the result of the increased use of fingerprint databases. If we already have a suspect and match his fingerprints to ones left in the crime scene, the probability of positive match is indeed quite low. But, if the suspect is not known, and a multi-million database is searched for a match, it is quite possible to find few well-matching fingerprints and declare the wrong person as a suspect.

In order to confirm the validity of fingerprint evidence in courts, it is desirable, as in the case of DNA evidence, to derive specific probabilities that two fingerprints belong to the same person. Ideally, an automatic algorithm would be used to report exact confidence numbers, and these numbers would be statistically verified by the experiments. Unfortunately, the current performance of automatic fingerprint matchers is still inferior to the performance of human experts, and we can not rely on them. Some recent research attempts to find a more precise fingerprint individuality models which would agree with the results of automatic fingerprint matchers. For example, Pankanti et al. [22] consider the model which accounts for the way fingerprint matchers try to find a transformation of one minutia set into another. But the results of experiments show that constructed model still does not have required precision.

The individuality research is an active part of biometrics research. With regards to fingerprints we expect the appearance of more advanced individuality models, which would take into account the statistical distributions of minutia and ridges, as well as nonlinear fingerprint deformations. With the proliferation of other biometrics and their 'latent' recordings, e.g. face, gait, speech, we expect the growth of research into their individuality as well.

5.5. Hardening of Biometrics

The *two-factor authentication*, relying on biometrics and traditional random key based authentication, is usually considered as a good approach to increase the security of the system. Indeed, it would be more difficult for intruder to obtain both means, fake biometrics and stolen key, in order to bypass the security of such system than the system relying on only one of those factors. Both factors can be kept separate; the authentication of the user might consist in first verifying the key and then verifying the biometrics. If key is incorrect or the confidence of biometric match is low the user is not authenticated.

At the same time there is a growing number of approaches trying to merge both factors together and construct so called *hardened biometrics* or *biohashing* methods. In such approaches, both during enrollment and during matching the biometric template is transformed using user-specific random key. The matching is performed using transformed biometrics, and significant increases in performance are usually reported. Here we present a simple example of such technique.

Suppose the biometric template is represented as a fixed length feature vector of length N, $x_1, \ldots, x_N$, and suppose $0 \leq x_i \leq 1$ for all i. Let the user-specific key to be a binary string of length N, $b_1, \ldots, b_N$. Let the biometric hardening to be the following operation: $x_i \rightarrow x_i + b_i * (N + 1)$. In this case, if two different users use different keys, then there will be index j, where b_j is 0 for one user and 1 for the other. The distance between corresponding transformed features will be at least N, and the total distance between two transformed templates (for example, assuming city-block distance) is at least N. It is also easy to see that the distance between any two templates transformed using same key will be less than N. So, apparently the presented hardening algorithm is able to achieve 0 FAR - 0 FRR error rates: genuine users, utilizing same key, will have matching distance between templates always less than N, and impostor users, utilizing different keys, will have matching distance always bigger than N. The hardening transformations might be more complex and deal with non-fixed biometric templates, but the essence remains

the same - biometrics of different users have different transformations and transformed templates have greater separation for impostors.

Does biometric hardening gives any advantage over separate use of biometrics and keys in two factor authentication systems? If we assume that genuine matches are always performed using same keys, and impostor matches always use different keys, the separate use of keys and biometrics can easily be made to have 0 FAR and 0 FRR - the matching should only compare keys and discard biometric matching scores. So, the claim of superior performance in hardened biometric systems is easily achieved when keys and biometrics are used separately. The interesting case would be if intruder steals the key of legitimate user and tries to be authenticated using this key. In separate key-biometrics system, the performance in this case will be exactly the performance of original biometric system. For hardened system we have some transformation which is applied to two templates of different persons; it is very doubtful that such transformation will result in better performance. If it were so, why would not we use so transformed biometric templates instead of original templates for original biometric matcher?

Thus, by considering different scenarios, hardened biometrics is expected to have worse performance than separate use of keys and biometrics in two-factor authentication systems [19]. Another point against biometric hardening is hiding of proper security analysis, which might involve the probabilities of either key or biometrics to be compromised. If deployed system will attempt to set acceptance thresholds so that claimed 0 FAR - 0 FRR performance is achieved, it will completely rely on keys (in order to make 0 FRR we have in general to accept any biometric match). The intruder with stolen key will be accepted by the system in this case.

It might be difficult for biometric system buyers to determine whether the claims of superior performance are results of improving matching algorithms or the results of hardening. Consequently, despite having worse performance and decreased security, it is possible that hardened biometric systems will be increasingly deployed in the future.

Note, that cancelable biometrics (section 5.1) is also a two-factor authentication system, and due to the effect described in this section, a superior performance for such systems might be claimed. In order to correctly estimate the performance of cancelable biometric system, we need to assume that intruder is able to steal the user-specific key. When the templates of different users use same key, the transformation applied to these templates is the same, and we expect the reduced matching performance of corresponding cancelable templates.

5.6. Performance of Biometric Matchers and Quality Control

Due to large commercial interests in the biometrics field there is a great number of reports claiming almost ideal performances of developed biometric systems. It is practically impossible to verify such reports - the systems might include expensive and difficult-to-obtain sensors and evaluations might be performed on privately collected data. The system's performance evaluation might also be distorted by the use of hardening, which as we discussed can elementarily make any biometric matcher to appear to have ideal performance.

The competitions using publicly available data and well-defined performance evaluation criteria provide a good way to compare the performance of different matching algorithms.

Fingerprint Verification Competitions (FVC), Face Recognition Vendor Test (FRVT) and Iris Challenge Evaluation (ICE) are the examples of such competitions. The testing protocols usually include multiple performance criteria for evaluating biometric matchers. For example, FVC competitions report EER, TER and FRR rates corresponding to different FAR levels (1%, .1%, .01% FAR). This is reasonable approach to performance evaluation - as we saw in section 3.2 a single number is not sufficient for comparison, and few selected numbers give an adequate replacement for comparisons of ROC curves.

As the results of recent competitions show [23], modern biometric matchers have achieved good progress. Though, the human visual system is well adapted for the task of face recognition, automated face matchers can have better performance than humans. Another conclusion of the experiments is the importance of good quality biometric scanners and standardized acquisition procedures. For example, the face recognizers perform best on high resolution face images taken under controlled illumination conditions.

The quality control during biometric scanning can be a decisive factor in the deployment of biometric system. The large-scale iris recognition system [9] deployed in UAE reportedly did not produced any errors during its entire operation. But the same iris matching algorithm had only average performance in ICE 2006 competition. This might be explained by the poor quality of some iris images in the ICE 2006 database. The quality control in the production biometric system might be able to detect the presence of such bad images and require additional scanning attempts.

6. Conclusion

The area of biometrics includes multiple topics and is currently under intensive study by many scientists and companies. In this chapter we reviewed the major topics of biometrics research. Some research topics have reached a maturity stage and are interesting mainly from implementation point of view. For example, multiple solutions have been proposed for fingerprint matching, and the problem consists in the proper combination of these solutions rather than in developing new algorithms. But, still there are topics which do not have ready solutions and present challenges. Cancelable biometrics, indexing and biometrics individuality are among such topics.

REFERENCES

1. .B. Ashraf, S. Lucey, and T. Chen. Learning patch correspondences for improved viewpoint invariant face recognition. In *IEEE International Conference on Computer Vision and Pattern Recognition (CVPR)*, 2008.
2. John Berry and David A. Stoney. History and development of fingerprints. In Henry C. Lee and R. E. Gaensslen, editors, *Advances in Fingerprint Technology.* CRC Press, 2001.
3. V. Blanz and T. Vetter. Face recognition based on fitting a 3d morphable model. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 25(9):1063–1074, 2003.
4. R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Fingerprint classification by directional image partitioning. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 21(5):402–421, 1999.

5. Sharat Chikkerur, Alexander N. Cartwright, and Venu Govindaraju. Fingerprint enhancement using STFT analysis. *Pattern Recognition*, 40(1):198–211, 2007.
6. T. Clancy, D. Lin, and N. Kiyavash. Secure smartcard-based fingerprint authentication. In *ACM Workshop on Biometric Methods and Applications (WBMA 2003)*, 2003.
7. Simon A. Cole. More than zero: Accounting for error in latent fingerprint identification. *Journal of Criminal Law and Criminology*, 95(3), 2005.
8. T.F. Cootes, G.J. Edwards, and C.J. Taylor. Active appearance models. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 23(6):681–685, 2001.
9. J. Daugman and I. Malhas. Iris recognition border-crossing system in the UAE. *International Airport Review*, (2), 2004.
10. John G. Daugman. High confidence visual recognition of persons by a test of statistical independence. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 15(11):1148–1161, 1993.
11. G. Davida, Y. Frankel, and B. Matt. On enabling secure applications through on-line biometric identification. In *Proc. of the IEEE 1998 Symp. on Security and Privacy*, Oakland, Ca., 1998.
12. Kresimir Delac, Mislav Grgic, and Sonja Grgic. Independent comparative study of PCA, ICA, and LDA on the FERET data set. *International Journal of Imaging Systems and Technology*, 15(5):252–260, 2005.
13. F. Farooq, R.M. Bolle, Tsai-Yang Jea, and N. Ratha. Anonymous and revocable fingerprint recognition. In R.M. Bolle, editor, *Computer Vision and Pattern Recognition, 2007. CVPR '07. IEEE Conference on*, pages 1–7, 2007.
14. F. Galton. *FingerPrints*. McMillan, 1892.
15. R.S. Germain, A. Califano, and S. Colville. Fingerprint matching using transformation parameter clustering. *Computational Science and Engineering, IEEE [see also Computing in Science & Engineering]*, 4(4):42–49, 1997.
16. Tsai-Yang Jea and Venu Govindaraju. A minutia-based partial fingerprint recognition system. *Pattern Recognition*, 38(10):1672–1684, 2005.
17. A. Juels and M. Sudan. A fuzzy vault scheme. In *IEEE International Symposium on Information Theory*, 2002.
18. J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas. On combining classifiers. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 20(3):226–239, 1998.
19. Adams Kong, King-Hong Cheung, David Zhang, Mohamed Kamel, and Jane You. An analysis of biohashing and its variants. *Pattern Recognition*, 39(7):1359–1368, 2006.
20. Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition*. Springer-Verlag, 2003.
21. Amit Mhatre, Sharat Chikkerur, and Venu Govindaraju. Indexing biometric databases using pyramid technique. In *Audio and Video-based Biometric Person Authentication (AVBPA)*, pages 841–849, 2005.
22. S. Pankanti, S. Prabhakar, and A.K. Jain. On the individuality of fingerprints. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(8):1010–1025, 2002.
23. P. Jonathon Phillips, W. Todd Scruggs, Alice J. OToole, Patrick J. Flynn, Kevin W.Bowyer, Cathy L. Schott, and Matthew Sharpe. FRVT 2006 and ICE 2006 large-

scale results. Technical Report NISTIR 7408, NIST, 2007.
24. Walter J. Scheirer and Terrance E. Boult. Cracking fuzzy vaults and biometric encryption. In Terrance E. Boult, editor, *Biometrics Symposium, 2007*, pages 1–6, 2007.
25. T. Sim, S. Baker, and M. Bsat. The CMU pose, illumination, and expression database. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 25(12):1615–1618, 2003.
26. Sergey Tulyakov, Faisal Farooq, Praveer Mansukhani, and Venu Govindaraju. Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, 28(16):2427–2436, 2007.
27. Sergey Tulyakov and Venu Govindaraju. Utilizing independence of multimodal biometric matchers. In *International Workshop on Multimedia Content Representation, Classification and Security*, Istanbul, Turkey, 2006.
28. Sergey Tulyakov, Venu Govindaraju, and Chaohong Wu. Optimal classifier combination rules for verification and identification systems. In *7th International Workshop on Multiple Classifier Systems*, Prague, Czech Republic, 2007.
29. Sergey Tulyakov, Chaohong Wu, and Venu Govindaraju. Iterative methods for searching optimal classifier combination function. In *First IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007.*, pages 1–5, 2007.
30. Matthew Turk and Alex Pentland. Eigenfaces for recognition. *J. Cognitive Neuroscience*, 3(1):71–86, 1991.