# Chapter 1
# Introduction

**Abstract** In biometric identification systems, the identity corresponding to an individual is determined by comparing his/her template against all user templates in the database. This exhaustive matching process increases the response time and the number of false matches of the system. An effective mechanism is required that reduces the number of templates to be compared with the query during identification. Biometric indexing is such technique that limits the search space and identifies an individual in real time with high accuracy. Many authors have presented a number of biometric indexing techniques. This chapter explores the fundamentals of biometric indexing, its challenges, classifying and benchmarking along with a number of techniques proposed by various researchers.

**Keywords** Biometrics · Verification · Identification · Indexing · Classification

## 1.1 Introduction

In today's security conscious society, automatic personal authentication is important in different applications including government, commercial, educational institutions, industries, public places, etc. Questions such as "Is this the person who he claims to be?", "Should this individual be authorized to perform this transaction?", "Does this employee have authorization to access this service?" etc., are asked millions of time every day by thousands of organizations in both private and public sectors [1].

Existing systems use either identity cards or passwords for personal authentication (Fig. 1.1a). These security systems no longer suffice for individual authentication because cards can be stolen or forged and a password can be forgotten or cracked. The following are some interesting statistics:

1. According to a report by Nilson, "$11.27 billion losses due to credit card and debit card fraud during 2012" [2].
2. According to American Bankers Association's Deposit Account Fraud Survey-2011, "Financial institutions incurred $955 million in losses due to debit card fraud in 2010, which is around a 21% increase from the $788 million in losses incurred during 2008" [2].



I. Kavati et al., *Efficient Biometric Indexing and Retrieval Techniques for Large-Scale Systems*, SpringerBriefs in Computer Science,
DOI 10.1007/978-3-319-57660-2_1

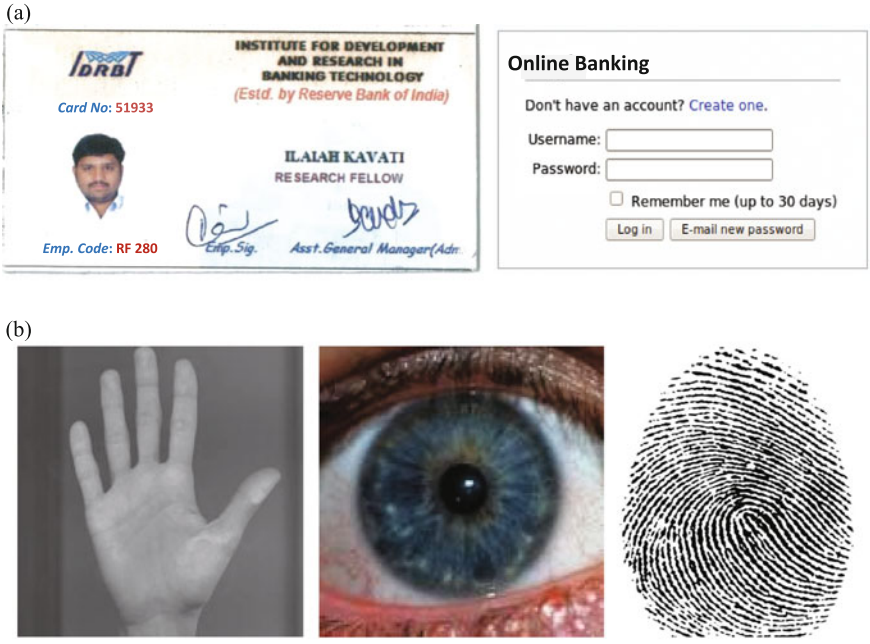


**Fig. 1.1** Personal authentication techniques: **a** Traditional methods such as identity cards, Passwords, etc., **b** Biometric characteristics [16]

3. According to the Gartner Group, "between 20 to 50% of all help desk calls are for password resets and the average help desk labor cost for a single password reset is about $70" [3].

The above statistics shows the need of an accurate and efficient approach for personal recognition. Biometric recognition that uses humans fingerprint and/or palmprint and/or iris, etc., is a better choice and a reliable solution for convenient human recognition (Fig. 1.1b). As humans biometric features are unique, cannot be stolen/forgotten, and the person must be physically present during authentication [4], biometric recognition systems are gaining popularity and deployed in many important applications [5–13]. This results large-scale biometric databases in real time and an identification system need to search millions of records to identify a query. As the biometric data do not have any natural sorting order like numeric or alphabetic [14, 15], recognition in these large biometric systems is a challenging problem. In this book, we explore methods that are capable of searching biometric databases in real time with a high level of confidence.

## 1.2 Biometric Recognition

"A biometric system is a pattern recognition system that recognizes individuals based on the measurement of their physiological and/or behavioral traits: Physiological traits include a person's fingerprint, facial features, palmprint, vein pattern, or ocular characteristics; Behavioral traits include voice, gait, keystrokes, signature etc." [17]. The word biometrics is derived from the Greek words bios (meaning life) and metron (meaning measurement), i.e., biometric traits are the measurements from living human body. Figure 1.2 shows a few of the biometric traits (including physiological and behavioral) for personal recognition.

A generic biometric system is shown in Fig. 1.3. It consists of two modules: enrollment and recognition.

### Enrollment

This module enrolls the individuals into the biometric system (Fig. 1.3a). During enrollment, a sensor captures the biometric characteristic of an individual, from which a set of features (template) are extracted by a feature extractor. Depending on the application context, the extracted feature template may be stored in a central database along with the individual's identity (name, ID number, etc.) or be recorded on a smart card issued to the individual.

### Recognition

This module recognizes the identity of an individual at the point of service. During this phase, the sensor acquires the biometric characteristic of the individual to be recognized. The captured biometric image is preprocessed by the feature extractor to generate the template. The extracted template is compared to the prestored template(s) using a matcher to establish the identity. The process of user recognition in biometric systems is shown in Fig. 1.3b, c. A biometric recognition system is designed to work in one of the two different modes: (i) verification or (ii) identification.

### *1.2.1 Verification*

In verification mode, the user will claim his identity by using a user name, or a personal identification number, or a smart card, etc., along with the biometric data. The system will then verify the user by matching the acquired biometric characteristic with his own biometric sample prestored in the system. The system in this mode, conducts a one-to-one matching to determine whether the identity claimed by the individual is true or not [18]. In this case, the question "Is Mr. X really who he claims to be?" is answered in either acceptance or rejection. An example of the verification scenario occurs when we try to use the ATM at a bank. We have to provide our biometric data along with ATM card to verify our identity. In this case, the system

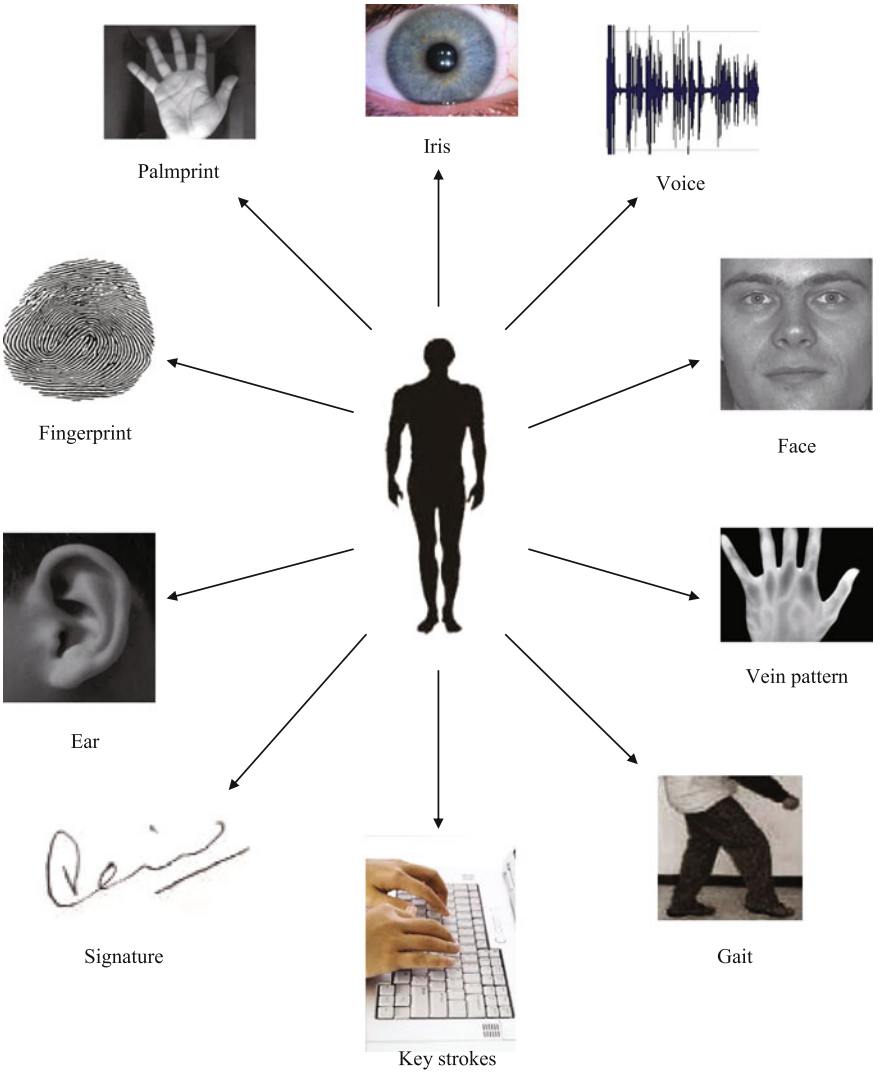


**Fig. 1.2** Different biometric traits for personal recognition

compares the provided biometric data with our prestored template to ensure that the true owner is the one who is using the card to perform the transaction. The process of recognizing a user in verification mode can be seen in Fig. 1.3b.

### 1.2.2 Identification

In this mode, the user does not claim any identity. The user provides his biometric data, and the data is compared to the stored template of every individual in the system database. The system in this mode, conducts a one-to-many comparison to find the identity of an individual. In this case, the question "To whom does the submitted biometric data belong?" is answered. For example, if a fingerprint impression is found at a crime scene, to determine the suspect it is compared to all the enrolled fingerprints in the database. If a match is found, the identity of the suspect is determined. The process of recognizing a user in identification mode can be seen in Fig. 1.3c.

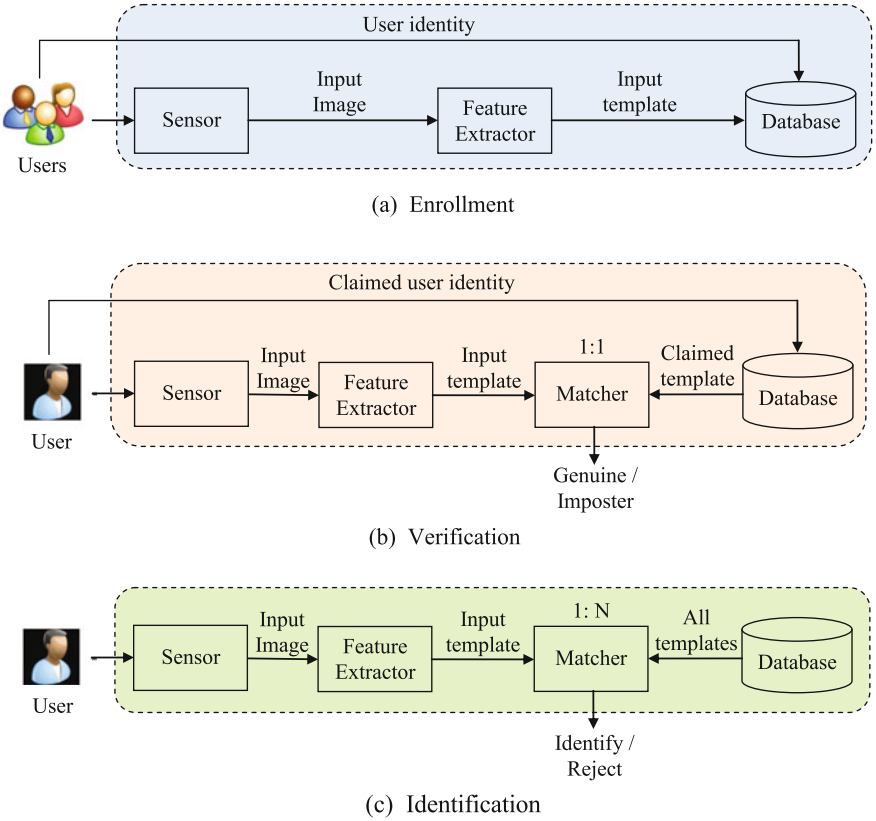


**Fig. 1.3** Different modes of operation of a generic biometric system [16]

## 1.3 Indexing

In today's security conscious society, biometric recognition systems became more popular and deployed in variety of applications such as surveillance, border control, network access, banking, employee authentication, etc. The market for biometric applications is growing worldwide, and specifically in emerging economies, such as India, where scalability is a huge challenge. According to a market research report by Acuity Market Intelligence (AMI) [19], the market for worldwide biometrics industry is expected to grow steadily from an annual revenue of 3.4 billion USD in 2009 to 11 billion USD in 2017 as shown in Fig. 1.4.

Note that, most of these biometric systems deal with large-scale databases and their size is increasing at a rapid pace. For instance, India's national ID program [5] called Unique Identification Authority of India (UIDAI) registered a database of 700 million people. It will reach 1.25 billion people in a few years and the number of accesses per day is expected to be 1 to 5 million. In the United States, Federal Bureau of Investigation (FBI) developed a fingerprint database called Integrated Automated Fingerprint Identification System (IAFIS) [20]. Currently, it has records of over 51 million criminals and over 1.5 million noncriminals.

However, identification of an individual in such large databases is typically determined by matching his/her biometric template with each enrolled template in the database. This is computationally expensive, i.e., response time increases linearly

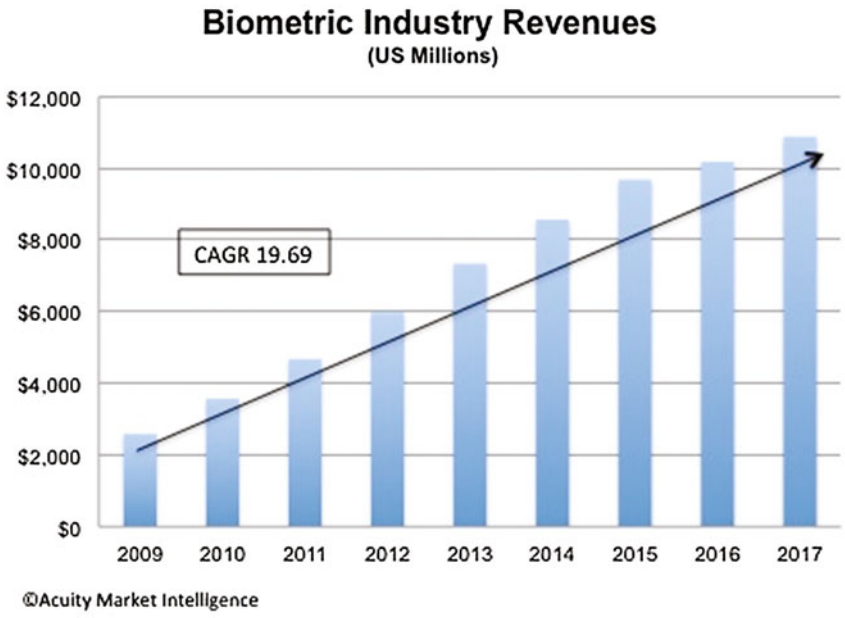


**Fig. 1.4** Acuity Market Intelligence (AMI) Report

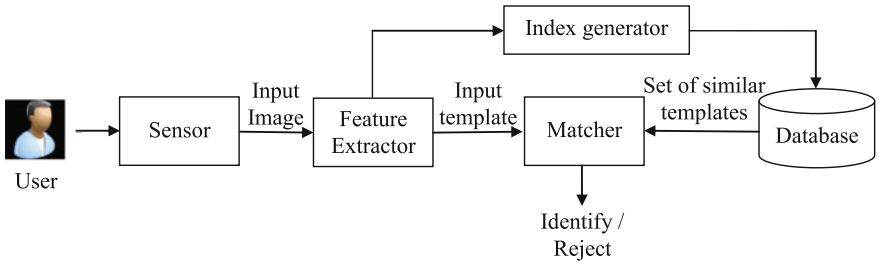


**Fig. 1.5** Process of Biometric identification using indexing approach [16]

with size of the database. Hence, there is a need of efficient retrieval methods that can enable searches in reduced space of the database and thus reduces the search time without compromising accuracy.

This ***problem***, i.e., ***search space reduction in biometric databases*** may be stated as follows: *Given a large biometric database D and a query q, the identification system has to*,

- Quickly retrieve a candidate set $C$ from $D$ such that the retrieved images in $C$ are most similar to $q$,
- $|C| \ll |D|$, and
- $C$ must contain $q$'s identity with high probability.

There are two different approaches to handle this problem. The first one is partitioning the images stored in the database [21]. The entire database is divided into small number of partitions, i.e., classes. To identify a query, first its class is determined and compared only with the candidates of that class to which the query belongs. However, this approach uses only predefined classes and the images are unevenly distributed among them resulting in variation in the system performance [4]. Further, the system must handle rejected templates carefully.

The second approach is indexing which computes an index to every individual (Fig. 1.5). To identify a query, this technique retrieves a set of similar candidates from the database whose index are most similar to it. Next the query is compared only with the retrieved similar candidates instead of with the complete database and thus reduces the search space.

### *1.3.1 Challenges*

The following are few issues that need to be considered while indexing.

- Intra-class variations, i.e., two images of the same user obtained at different time instances may not be same. This is mainly because of,

  - Different sensors at different times.
  - Poor maintenance of sensors.
  - Changes in lighting conditions.
  - Lack of user cooperation. For example, a person may have beard or glasses at enrollment time but not at identification time; different facial expressions at different times.

  This may increase the false rejections of the system as different indexes are possible for the same user.
- Inter-class similarity, i.e., overlap of feature space of different users leads to increase in false matches.
- Further, indexing methods of relational databases are also not suitable for biometric data [14, 15]. In relational databases, records (or data) are arranged in an alphabetical or numerical order with respect to a primary key for efficient retrieval. But biometric templates do not have any sorting order to arrange [14, 15].
- Finally, the indexing methods for multimedia (i.e., image, video) databases are also not suitable for biometric databases [22–31]. The following are a few reasons:

  - In multimedia databases, there is large variability among the subjects in terms of appearance i.e., different type of subjects (like trees, humans, buildings, etc.) are present in the database. Hence, a coarse-level classification is possible. But, there is little appearance variability among the biometric images of different users, i.e., the biometric samples of different users look almost similar. For example, in a fingerprint database, the impressions of different users almost look similar with few differences.
  - The multimedia (especially image and video) data are represented with metadata [31] such as annotated text, symbols, tags, etc., which is not possible for biometric data.
  - Finally, the feature representation of biometric data is different from multimedia data [32]. Basically, the multimedia data is represented with texture [24, 27–29], color [22, 23, 25] and shape [26] features. However, most of the biometric characteristics do not contain these features.

## 1.4 Biometric Indexing Techniques

The fast identification in biometric databases can be achieved by two different approaches: classification and indexing. These approaches are used to filter the search space during identification process. In classification approaches, the database images are divided into different groups (classes) such that the images in the same class are similar in terms of some quantitative information. During identification, the class of the query is first identified and then it is matched with only the images present in that class. However, as said earlier, these approaches have a serious limitation that the images are unevenly distributed among the predefined classes which makes the system statistically unreliable for faster identification.

In indexing approaches, each image is assigned an index based on its features. During identification, the query is matched with only the images which have similar index. Majority of current developments for biometric indexing are based on one of the following features:

1. Key feature points [33–42]
2. Geometric properties of Triplets [18, 43–48]
3. Match scores [49–54]
4. Other approaches
   - Ridge orientation based (for fingerprint) [55–58]
   - Texture based (for palmprint [59–62], iris [32, 63, 64])
   - Color based (for iris) [65–67]
   - Subspace approximations (for face) [68–70].

### *1.4.1 Key Feature Point Based Indexing Approaches*

These approaches extract the key feature points from the biometric samples and use them for indexing purpose. Boro et al. [33] developed an indexing technique using fingerprint minutiae points (i.e., bifurcation and end points). The minutiae features are enrolled into a hash table using geometric hashing [71]. Jayaraman et al. [36] proposed a minutiae-based geometric hashing technique for fingerprint indexing. A fixed length feature vector called Minutiae Binary Code (MBC) is computed for each minutia in the fingerprint. The minutiae and its feature vector are stored into the hash table using geometric hashing.

Mansukhani et al. proposed an indexing approach based on minutiae tree [34]. They constructed a large index tree where the enrolled templates are represented by the leaves of the tree. The branches in the index tree correspond to different local configurations of minutiae points. Searching the index tree entails extracting local minutiae neighborhoods of the test fingerprint and matching them against tree nodes. Cappelli et al. developed Minutiae Cylinder-Code (MCC) based indexing technique [35]. For each fingerprint, a fixed size binary code is computed. This code is a representation of spatial and directional relationships between a minutia and its neighborhood structure with a minutiae cylinder. To find the best matches, Locality Sensitive Hashing (LSH) technique is used.

Badrinath et al. [37] propose an efficient indexing scheme using geometric hashing of Speeded Up Robust Features (SURF) [72] to index the palmprint into a hash table. During querying, a score-level fusion of voting strategy based on geometric hashing and SURF score is used to identify the live palmprint. In a recent work, Dewangan et al. [39] proposes a face indexing method based on SURF key features and *k-d* tree. Authors created a two-level index space based on the SURF key points and divide the index space into a number of cells. Further, they define a set of hash functions to store the SURF descriptors of a face image into the cell. The SURF descriptors within an index cell are stored into *k-d* tree.

**Table 1.1** Key feature point based indexing approaches

| Author | Features used | Approach | Biometric |
|---|---|---|---|
| Boro and Roy (2004), [33] | Minutiae features | Geometric hashing | Fingerprint |
| Jayaraman et al. (2014) [36] | Minutiae features | Geometric hashing and Minutiae binary code | Fingerprint |
| Mansukhani et al.(2010), [34] | Minutiae features | Minutiae tree | Fingerprint |
| Cappelli et al. (2010), [35] | Minutiae features | Minutiae cylinder-code and Locality sensitive hashing | Fingerprint |
| Badrinath et al. (2013), [37] | SURF features | Geometric hashing and fusion | Palmprint |
| Dewangan et al. (2013), [39] | SURF features | *kd*- tree | Face |
| Mehrotra et al. (2010), [40] | SIFT features | Geometric hashing | Iris |
| Panda et al. (2013), [41] | SIFT features | Parallel geometric hashing | Iris |
| Mehrotra et al. (2013), [42] | SIFT features | *k–d–b* tree | Iris |

Mehrotra et al. [40] proposed an indexing method based on Scale Invariant Feature Transform (SIFT) [73]. The SIFT features are extracted for each iris image and mapped into a hash table using geometric hashing. Panda et al. [41] proposed an indexing method for iris databases using parallel geometric hashing. Authors first, extract the SIFT features from the iris images. The SIFT features are indexed into a hash table using a parallel geometric hashing using multiple processors. The use of parallel processors increases the retrieval performance of the system during identification. In another work, Mehrotra et al. [42] also used the SIFT features for iris indexing. The extracted SIFT features are indexed using a *k-d-b* tree. During identification, a range search is used to retrieve a set of similar images to the query. The summary of different key feature point based indexing techniques is given Table 1.1.

### *1.4.2 Triplet-Based Indexing Approaches*

These approaches compute some form of triplets using the feature points of the biometric samples for indexing purpose. Bhanu and Tan [43] proposed a triplet-based fingerprint indexing method. They compute all the possible triplets from the extracted minutiae of a fingerprint. Their method used triangle features such as handedness, type, direction, etc. to compute the index. Instead of all possible triangulation, Bebis et al. used Delaunay triangulation [74] of minutiae points for indexing fingerprints [44]. For each triplet of the fingerprint, their method computes the ratios of largest side of the triplet with the two smallest sides and the angle between the smallest sides to generate the index.

Ross and Mukherjee [45] also developed an indexing technique based on Delaunay triangles. However, they added ridge curvature to the minutiae triplets for improved performance. Further, they used $k$-means clustering for indexing the triplets. Another Delaunay triangulation-based indexing approach was proposed by Liang et al. [18]. However, this approach uses lower order Delaunay triangulation [75]. They proved that the Delaunay triangulation is sensitive to skin distortion and the order-0, order-1 Delaunay triangles are more stable and robust against distortion. Further, Alonso et al. [46] extended the Delaunay triangulation to handle the distortions caused by spurious and missing minutiae. Iloanusi et al. [48] proposed a minutiae quadruplet based approach for fingerprint indexing. The authors used multiple fingers of an individual and extracted the geometric information from the minutiae quadruplets. Four, five, and ten fingerprints from a subject are fused at the rank level using the highest rank rule.

Jayaraman et al. [47] also proposed a method for palmprint indexing using SURF features. They extract the SURF features from each palm image. Then they apply a series of preprocessing steps on the SURF features, such as, mean centering, principal component analysis, rotation, and normalization to make them invariant to affine transformations. Finally, a block-based triangulation is applied and the geometric features of the triangles are indexed using geometric hashing. Table 1.2 shows the summary of various triplet-based indexing approaches.

### *1.4.3 Match Score Based Indexing Approaches*

These approaches use the match score between the images for indexing purpose. The first such attempt was made by Maeda et al. [49]. A match score vector was calculated for each image by matching it against all the images in the database and stored. During identification, the match score vector of the query is compared against each image score vector.

**Table 1.2** Triplet-based indexing approaches

| Author | Features used | Approach | Biometric |
|---|---|---|---|
| Bhanu and Tan (2003), [43] | Minutiae triplets | All possible triangle | Fingerprint |
| Bebis et al. (1999), [44] | Minutiae triplets | Delaunay triangulation | Fingerprint |
| Ross and Mukherjee (2007), [45] | Minutiae triplets and ridge curvature | $k$- means clustering | Fingerprint |
| Liang et al. (2007), [18] | Minutiae neighborhood and minutiae triplets | Delaunay triangulation | Fingerprint |
| Alonso et al. (2013), [46] | Minutiae triplets | Extended triangulation | Fingerprint |
| Iloanusi et al. (2014), [48] | Minutiae quadruplets | Clustering | Fingerprint |
| Jayaraman et al. (2013), [47] | Triangulation of normalized SURF features | Modified geometric hashing | Palmprint |

**Table 1.3** Match score based indexing approaches

| Author | Features used | Approach | Biometric |
|---|---|---|---|
| Maeda et al. (2004), [49] | Match score | Linear search | Fingerprint |
| Gyaourova and Ross (2012), [51] | Match scores | Linear search and correlation | Multimodal (Face, Fingerprint) |
| Paliwal et al. (2010), [52] | Match scores | VA+ file | Palmprint |
| Kavati et al. (2014a), [53] | Match scores | Voting | Palmprint |
| Kavati et al. (2014b), [54] | Match scores | Voting and leader clustering | Palmprint |

Gyaourova and Ross [51] present an indexing approach based on match scores. This method generates a set of match scores called index code, by comparing a biometric image with a small set of reference images. During querying, the match scores between the test image and all the enrolled images are compared to identify the candidate list. This approach was tested individually on face and fingerprint database. Finally, the candidate identities from both the databases are fused to identify the best matches. Authors claim that comparison of two score vectors takes less time compared to matching two templates.

Paliwal et al. [52] proposed another work based on match scores. For each image, a set of match scores are computed like Gyaourova and Ross [51] method. The computed match scores are stored into a Vector Approximation (VA+) file which is a space partitioning method. This method use $k$-NN search and texture to retrieve top $k$ similar matches. This approach was tested on a palmprint database. Table 1.3 shows the summary of the various score based indexing approaches.

### *1.4.4 Other Indexing Approaches*

In the literature, there are also some indexing techniques for biometric systems which are based on different features other than discussed above. For example, ridge information for fingerprints; texture, color information for palmprints, iris and face biometrics, etc. Summary of other indexing techniques in the literature are given in Table 1.4.

## 1.5 Benchmarking in Indexing and Performance Evaluation

Benchmarking is the process of validating the results and comparing with already existing best practices in the literature. The benchmarking improves the quality of the development activity. Some of the biometric benchmark databases (like PolyU palm-

**Table 1.4** Other indexing approaches

| Author | Features used | Approach | Biometric |
|---|---|---|---|
| Lumini et al. (1997), [55] | Reduced dimensional directional image | K-L transform and continuous classification | Fingerprint |
| Lee et al. (2005), [56] | Ridge orientation, interridge spacing | Feature map and PCA | Fingerprint |
| Jiang et al. (2006), [57] | Ridge orientation, dominant ridge distance | Hierarchical based | Fingerprint |
| Cappelli (2011), [58] | Ridge orientation and ridge line frequencies | Weighted fusion of scores | Fingerprint |
| You et al. (2002), [59] | Global texture energy and interesting points | Multifeature hierarchical | Palmprint |
| You et al. (2004), [60] | Global texture energy, fuzzy interest line and local directional texture energy features | Multifeature coding based | Palmprint |
| Li et al. (2005), [61] | Global texture energy and local texture energy | Multifeature hierarchical | Palmprint |
| Mukherjee and Ross (2008), [63] | Gabor wavelet IrisCode features | PCA and $k$-means clustering | Iris |
| Mehrotra et al. (2009), [64] | DCT energy histogram features | B-tree | Iris |
| Dey et al. (2012), [32] | Gabor energy features | Hashing | Iris |
| Fu et al. (2005), [65] | Maximum response from an artificial color filter | Color based classification | Iris |
| Puhan and Sudha (2008), [66] | Blue and red color indices | Color based classification | Iris |
| Jayaraman et al. (2012), [67] | Color and SURF features | kd-tree | Iris |
| Kyperountas et al. (2008), [68] | Discriminant projected face data | Clustering | Face |
| Lin et al. (2003), [69] | Eigenfaces and PCA | Condensed database | Face |
| Mohanty et al. (2008), [70] | Linear subspace based match scores | $k$-NN search | Face |

print, FVC fingerprint) are available to the research community for evaluation. The performance of the indexing algorithm can be calculated based on various parameters like hit rate and penetration rate.

## *1.5.1 Databases*

Experiments are conducted on the following biometric databases:

1. Fingerprint Verification Competition (FVC) databases
2. PolyU Palmprint database

These databases exhibit some fundamental differences such as type of biometric, device used to capture the images, resolution, lighting conditions, etc. This forms the basis for the study of the proposed work under different circumstances. Detailed description of these databases is given in the following:

### 1.5.1.1 Fingerprint Verification Competition (FVC) Databases

The seven FVC databases used in the experiments are: 1. FVC 2002 DB1, 2. FVC 2002 DB2, 3. FVC 2002 DB3, 4. FVC 2002 DB4, 5. FVC 2004 DB1, 6. FVC 2004 DB2, and 7. FVC 2004 DB4. Each of these database comprises images from 100 different fingers. Each finger has 8 impressions in the database. This makes a total of 800 images to perform the experiments. Further, each database is divided into two mutually exclusive training (i.e., $Gallery$) and test (i.e., $Probe$) sets. Arbitrarily, four images per finger are chosen for training and the remaining four images are used for testing.

### 1.5.1.2 PolyU Palmprint Database

The PolyU palmprint database was acquired at the Hong Kong Polytechnic University using a CCD (Charge Coupled Device) camera [76] at a spatial resolution of 75 dpi and 256 gray levels. This benchmark database consists of 7,752 grayscale images of size $384 \times 284$ pixels corresponding to 386 different palms. Around 20 images per palm have been collected in two sessions. Arbitrarily 10 images per palm are considered for training and remaining 10 images are used for testing. Table 1.5 shows the detailed description of each database used in the experiments.

## *1.5.2 Performance Metrics*

The performance of the proposed indexing approaches is determined using the following measures:

**Table 1.5** Characteristics of the databases used in the experiments

| Database | Size | Sensor | Image size | Subjects | Samples | Resolution (dpi) |
|---|---|---|---|---|---|---|
| FVC 2002 DB1 | 800 | Optical sensor | 388 × 374 | 100 | 8 | 500 |
| FVC 2002 DB2 | 800 | Optical sensor | 296 × 560 | 100 | 8 | 569 |
| FVC 2002 DB3 | 800 | Capacitive sensor | 300 × 300 | 100 | 8 | 500 |
| FVC 2002 DB4 | 800 | Synthetic | 288 × 384 | 100 | 8 | ≈500 |
| FVC 2004 DB1 | 800 | Optical sensor | 640 × 480 | 100 | 8 | 500 |
| FVC 2004 DB2 | 800 | Optical sensor | 328 × 364 | 100 | 8 | 500 |
| FVC 2004 DB4 | 800 | Synthetic | 288 × 384 | 100 | 8 | ≈500 |
| PolyU palmprint | 7752 | CCD camera | 384 × 284 | 386 | ≈20 | 75 |

1. Hit Rate (HR)
2. Miss Rate (MR)
3. Penetration Rate (PR)
4. Cumulative Match Characteristics (CMC) curve

#### 1.5.2.1 Hit Rate (HR):

Hit Rate (HR) is the percentage of test set images for which the corresponding gallery set image with the correct match is present in the retrieved candidate set.

$$HR = \left(\frac{y}{M}\right) \times 100\% \tag{1.1}$$

where $y$ is the correctly identified test set images and $M$ is the total number of test set images.

#### 1.5.2.2 Miss Rate (MR):

Miss Rate (MR) is the percentage of probe set images for which the corresponding gallery set image with the correct match is not present in the candidate set.

$$MR = 100 - HR \tag{1.2}$$

#### 1.5.2.3 Penetration Rate (PR):

Penetration Rate (PR) is the average percentage of gallery set images retrieved (i.e., Candidate set) to identify a query image from the test set by the indexing mechanism.

$$PR = \left( \frac{1}{M} \sum_{i=1}^{M} \frac{|C^i|}{N} \right) \times 100\% \tag{1.3}$$

where $C^i$ is the candidate set of the $i^{th}$ test set image, $N$ is the number of images in the gallery set, and $M$ is number of images in the test set.

An efficient indexing method will have a high hit rate (low miss rate) and a low penetration rate.

#### 1.5.2.4 Cumulative Match Characteristics (CMC) Curve

CMC curves represent the identification accuracy of the system at various ranks. To determine the accuracy, the images in the retrieved candidate set are sorted in descending order such that the image in the first position is most similar to the query and other positions are arranged accordingly. We assign rank 1 to the image in candidate set at the first position, rank 2 to the image at the second position, and so on. Accuracy at rank $n$ (denoted by $I_n$) indicates the percentage of test set images for which the genuine match is present in top $n$ images of the sorted candidate set. This is formulated in Eq. 1.4, where $z$ denote the number of test set images for which the genuine match is in top $n$, and $M$ denote the total number of images in the test set.

$$I_n = \frac{z}{M} \tag{1.4}$$

## 1.6 Summary

The chapter includes a brief introduction to biometric recognition and importance of indexing. It also explored different issues that should be addressed by an indexing system. The current developments in the field of biometric indexing and retrieval also explored. Finally the benchmarking, and performance evaluation procedures for biometric indexing techniques are explained.

## References

1. A.K. Jain, P. Flynn, and A. Ross. *Handbook of biometrics*. Springer, 2007.
2. **Credit Card and Debit Card Fraud Statistic**. http://www.cardhub.com/edu/credit-debit-card-fraud-statistics, May 2014.
3. **Password Cost Estimater**. http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm, May 2014.
4. D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer, 2nd edition, 2009.
5. AADHAAR. **Unique Identification Authority of India**. http://uidai.gov.in/, July 2014.

6. **Singapore Immigration and Checkpoint authority**. http://www.ica.gov.sg/page.aspx?pageid=407, september 2014.
7. CROSSING U.S. BORDERS. http://www.dhs.gov/crossing-us-borders, July 2014.
8. FIND BIOMETRICS. **Mobile Biometrics, PDAs & Laptop Fingerprint Readers**. http://findbiometrics.com/applications/mobile-biometrics/, september 2014.
9. PLANET BIOMETRICS. **Physical Access and Attendence**. http://www.planetbiometrics.com/physical-access/, september 2014.
10. **Iris Scans at Amsterdam Airport Schiphol**. http://www.schiphol.nl/Travellers/AtSchiphol/Privium/Privium/IrisScans.htm, september 2014.
11. **United Arab Emirates Deployment of Iris Recognition:**. http://www.cl.cam.ac.uk/~jgd1000/deployments.html, July 2014.
12. TSA. **Transportation Security Administration**. http://www.tsa.gov/, september 2014.
13. J. HAMMOND. **Biometric traveler screening introduced in Orlando, Denver next**. http://www.examiner.com/article/biometric-traveler-screening-introduced-orlando-denver-next/, september 2014.
14. A. MHATRE, S. PALLA, S. CHIKKERUR, AND V. GOVINDARAJU. **Efficient search and retrieval in biometric databases**. In *Society of Photo-Optical Instrumentation Engineers proceedings series*, pages 265–273, 2005.
15. A. MHATRE, S. CHIKKERUR, AND V. GOVINDARAJU. **Indexing biometric databases using pyramid technique**. In *Audio-and Video-Based Biometric Person Authentication*, pages 841–849, 2005.
16. ILAIAH KAVATI, MUNAGA VNK PRASAD, AND CHAKRAVARTHY BHAGVATI. **Search Space Reduction in Biometric Databases: A Review**. *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention*, page 236, 2016.
17. A.K. JAIN, A. ROSS, AND K. NANDAKUMAR. *Introduction to biometrics*. Springer, 2011.
18. X. LIANG, A BISHNU, AND T. ASANO. **A Robust Fingerprint Indexing Scheme Using Minutia Neighborhood Structure and Low-Order Delaunay Triangles**. *IEEE Transactions on Information Forensics and Security*, **2**(4):721–733, 2007.
19. ACUITY. **The Future of Biometrics Market Research Report**. http://www.acuitymi.com/FOBReport.php, september 2014.
20. FBI. **Integrated Automated Fingerprint Identification System**. http://www.fbi.gov/about-us/cjis/fingerprintsbiometrics/iafis/iafis, september 2014.
21. E. HENRY. *Classification and Uses of Finger Prints*. Routledge, London, 1900.
22. G.H. LIU AND J.Y. YANG. **Content-based image retrieval using color difference histogram**. *Pattern Recognition*, **46**(1):188–198, 2013.
23. Y. D. CHUN, N. C. KIM, AND I. H. JANG. **Content-Based Image Retrieval Using Multiresolution Color and Texture Features**. *IEEE Transactions on Multimedia*, **10**(6):1073–1084, 2008.
24. H.A. MOGHADDAM AND M.N. DEHAJI. **Enhanced Gabor wavelet correlogram feature for image indexing and retrieval**. *Pattern Analysis and Applications*, **16**(2):163–177, 2013.
25. J. HUANG, S.R. KUMAR, M. MITRA, W.J. ZHU, AND R. ZABIH. **Image Indexing Using Color Correlograms**. In *Proceedings of the Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 762–768, 1997.
26. S. BERRETTI, A.D. BIMBO, AND P. PALA. **Retrieval by Shape Similarity with Perceptual Distance and Effective Indexing**. *IEEE Transactions on Multimedia*, **2**(4):225–239, 2000.
27. M.K. MANDAL, T. ABOULNASR, AND S. PANCHANATHAN. **Fast wavelet histogram techniques for image indexing**. In *Proceedings of IEEE Workshop on Content-Based Access of Image and Video Libraries*, pages 68–72, Jun 1998.
28. H.A MOGHADDAM AND M.S. TARZJAN. **Gabor Wavelet Correlogram Algorithm for Image Indexing and Retrieval**. In *18th International Conference on Pattern Recognition*, **2**, pages 925–928, 2006.
29. B. S. MANJUNATH AND W. Y. MA. **Texture Features for Browsing and Retrieval of Image Data**. *IEEE Trans. Pattern Anal. Mach. Intell.*, **18**(8):837–842, 1996.

30. J. VLEUGELS AND R.C. VELTKAMP. **Efficient image retrieval through vantage objects**. *Pattern Recognition*, **35**(1):69–80, 2002.
31. J. JEON, V. LAVRENKO, AND R. MANMATHA. **Automatic Image Annotation and Retrieval Using Cross-media Relevance Models**. In *International ACM SIGIR Conference on Research and Development in Informaion Retrieval*, pages 119–126, 2003.
32. S. DEY AND D. SAMANTA. **Iris data indexing method using gabor energy features**. *IEEE Transactions on Information Forensics and Security*, **7**(4):1192–1203, 2012.
33. R. BORO AND S.D. ROY. **Fast and Robust Projective Matching for Fingerprints Using Geometric Hashing**. In *Indian Conference on Computer Vision, Graphics and Image Processing*, pages 681–688, 2004.
34. P. MANSUKHANI, S. TULYAKOV, AND V. GOVINDARAJU. **A Framework for Efficient Fingerprint Identification Using a Minutiae Tree**. *IEEE Systems Journal*, **4**(2):126–137, 2010.
35. R. CAPPELLI, M. FERRARA, AND D. MALTONI. **Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition**. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **32**(12):2128–2141, 2010.
36. U. JAYARAMAN, A.K. GUPTA, AND P. GUPTA. **An efficient minutiae based geometric hashing for fingerprint database**. *Neurocomputing*, **137**:115–126, 2014.
37. G.S. BADRINATH, P. GUPTA, AND H. MEHROTRA. **Score level fusion of voting strategy of geometric hashing and SURF for an efficient palmprint-based identification**. *Journal of real-time image processing*, **8**(3):265–284, 2013.
38. V.D. KAUSHIK, U. JAYARAMAN, A.K. GUPTA, A.K. GUPTA, AND P. GUPTA. **An efficient indexing scheme for face database using modified geometric hashing**. *Neurocomputing*, **116**:208–221, 2013.
39. J. DEWANGAN, S. DEY, AND D. SAMANTA. **Face Images Database Indexing for Person Identification Problem**. *International Journal of Biometrics and Bioinformatics*, **7**(2):93–122, 2013.
40. H. MEHROTRA, B. MAJHI, AND P. GUPTA. **Robust iris indexing scheme using geometric hashing of SIFT keypoints**. *Journal of Network and Computer Applications*, **33**(3):300–313, 2010.
41. A.C. PANDA, H. MEHROTRA, AND B. MAJHI. **Parallel geometric hashing for robust iris indexing**. *Journal of real-time image processing*, **8**(3):341–349, 2013.
42. H. MEHROTRA AND B. MAJHI. **An efficient indexing scheme for iris biometric using kdb trees**. In *Intelligent Computing Theories and Technology*, pages 475–484. 2013.
43. B. BHANU AND X. TAN. **Fingerprint indexing based on novel features of minutiae triplets**. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **25**(5):616–622, 2003.
44. G. BEBIS, T. DEACONU, AND M. GEORGIOPOULOS. **Fingerprint Identification Using Delaunay Triangulation**. In *International Conference on Information, Intelligence, and Systems*, pages 452–452, 1999.
45. A. ROSS AND R. MUKHERJEE. **Augmenting ridge curves with minutiae triplets for fingerprint indexing**. In *Defense and Security Symposium*, pages 65390C–65390C. International Society for Optics and Photonics, 2007.
46. A.G. ALONSO, J.H. PALANCAR, E.R. REINA, AND A.M. BRISEO. **Indexing and retrieving in fingerprint databases under structural distortions**. *Expert Systems with Applications*, **40**(8):2858–2871, 2013.
47. U. JAYARAMAN, S. PRAKASH, AND P. GUPTA. **Use of geometric features of principal components for indexing a biometric database**. *Mathematical and Computer Modelling*, **58**(1):147–164, 2013.
48. O.N. ILOANUSI. **Fusion of finger types for fingerprint indexing using minutiae quadruplets**. *Pattern Recognition Letters*, **38**:8–14, 2014.
49. T. MAEDA, M. MATSUSHITA, AND K. SASAKAWA. **Characteristics of the Identification Algorithm Using a Matching Score Matrix**. In *ICBA*, pages 330–336, 2004.
50. A. GYAOUROVA AND A. ROSS. **A novel coding scheme for indexing fingerprint patterns**. In *Structural, Syntactic, and Statistical Pattern Recognition*, pages 755–764. 2008.

51. A. Gyaourova and A. Ross. **Index Codes for Multibiometric Pattern Retrieval**. *IEEE Transactions on Information Forensics and Security*, **7**(2):518–529, 2012.
52. A. Paliwal, U. Jayaraman, and P. Gupta. **A score based indexing scheme for palmprint databases**. In *International Conference on Image Processing*, pages 2377–2380, 2010.
53. Munaga V N K Prasad Ilaiah Kavati and Chakravarthy Bhagvati. **An Efficient Coding Method for Indexing Hand Based Biometric Databases**. In *International Conference on Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, pages 723–731, 2014.
54. Munaga V N K Prasad Ilaiah Kavati and Chakravarthy Bhagvati. **A New Indexing Method for Biometric Databases using Match Scores and Decision-Level Fusion**. In *International Conference on Advanced Computing, Networking and Informatics*, pages 493–500, 2014.
55. A. Lumini, D. Maio, and D. Maltoni. **Continuous versus exclusive classification for fingerprint retrieval**. *Pattern Recognition Letters*, **18**(10):1027–1034, 1997.
56. S.O. Lee, Y.G. Kim, and G.T. Park. **A Feature Map Consisting of Orientation and Inter-ridge Spacing for Fingerprint Retrieval**. In *5th International Conference on Audio- and Video-Based Biometric Person Authentication*, pages 184–190, 2005.
57. X. Jiang, M. Liu, and A.C. Kot. **Fingerprint Retrieval for Identification**. *IEEE Transactions on Information Forensics and Security*, **1**(4):532–542, 2006.
58. R. Cappelli. **Fast and accurate fingerprint indexing based on ridge orientation and frequency**. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, **41**(6):1511–1521, 2011.
59. J. You, W. Li, and D. Zhang. **Hierarchical palmprint identification via multiple feature extraction**. *Pattern recognition*, **35**(4):847–859, 2002.
60. J. You, W.K. Kong, D. Zhang, and K.H. Cheung. **On hierarchical palmprint coding with multiple features for personal identification in large databases**. *IEEE Transactions on Circuits and Systems for Video Technology*, **14**(2):234–243, 2004.
61. W. Li, J. You, and D. Zhang. **Texture-based palmprint retrieval using a layered search scheme for personal identification**. *IEEE Transactions on Multimedia*, **7**(5):891–898, 2005.
62. F. Yue, W. Zuo, D. Zhang, and B. Li. **Fast palmprint identification with multiple templates per subject**. *Pattern recognition letters*, **32**(8):1108–1118, 2011.
63. R. Mukherjee and A. Ross. **Indexing iris images**. In *International Conference on Pattern Recognition*, pages 1–4, 2008.
64. H. Mehrotra, G.S. Badrinath, B. Majhi, and P. Gupta. **Indexing iris biometric database using energy histogram of DCT subbands**. In *Contemporary Computing*, pages 194–204. 2009.
65. J. Fu, H.J. Caulfield, S.M. Yoo, and V. Atluri. **Use of artificial color filtering to improve iris recognition and searching**. *Pattern Recognition Letters*, **26**(14):2244–2251, 2005.
66. N.B. Puhan and N. Sudha. **A novel iris database indexing method using the iris color**. In *Conference on Industrial Electronics and Applications*, pages 1886–1891, 2008.
67. U. Jayaraman, S. Prakash, and P. Gupta. **An efficient color and texture based iris image retrieval technique**. *Expert Systems with Applications*, **39**(5):4915–4926, 2012.
68. M. Kyperountas, A. Tefas, and I. Pitas. **Dynamic training using multistage clustering for face recognition**. *Pattern Recognition*, **41**(3):894–905, 2008.
69. K.H Lin, K.M. Lam, X. Xie, and W.C. Siu. **An efficient human face indexing scheme using eigenfaces**. In *International Conference on Neural Networks and Signal Processing*, **2**, pages 920–923, 2003.
70. P. Mohanty, S. Sarkar, R. Kasturi, and P.J. Phillips. **Subspace Approximation of Face Recognition Algorithms: An Empirical Study**. *IEEE Transactions on Information Forensics and Security*, **3**(4):734–748, 2008.
71. Y. Lamdan and H.J. Wolfson. **Geometric hashing: A general and efficient model-based recognition scheme**. In *ICCV*, **88**, pages 238–249, 1988.

72. H. BAY, T. TUYTELAARS, AND LUC VAN GOOL. **Surf: Speeded up robust features**. In *Computer Vision–ECCV*, pages 404–417. 2006.
73. D.G. LOWE. **Distinctive Image Features from Scale-Invariant Keypoints**. *International Journal of Computer Vision*, **60**(2):91–110, 2004.
74. M.D. BERG, M.V. KREVELD, M. OVERMARS, AND O.C. SCHWARZKOPF. *Computational geometry*. Springer, 2000.
75. M. ABELLANAS, P. BOSE, J. GARCÍA-LÓPEZ, F. HURTADO, M. NICOLÁS, AND P.A. RAMOS. **On properties of higher-order Delaunay graphs with applications**. In *Europian Workshop on Computational Geometry*, pages 119–122, 2005.
76. M. WONG, D. ZHANG, W.K. KONG, AND G. LU. **Real-time palmprint acquisition system design**. *IEE Proceedings Vision, Image and Signal Processing,*, **152**(5):527–534, 2005.