A Multibiometric Recognition System : Categorization, Retrieval Techniques & Applications

Kshama Dwivedi, Sachin Singh Thakur, Mayur Shishupal, Aarti Bhirud

***Abstract*— Reliable human authentication schemes are of paramount importance in our highly networked society. The multi-biometric recognition system enhances the performance and accuracy by consolidating the benefits of various uni-modal biometric systems. They are expected to meet the stringent performance requirements imposed by large-scale authentication systems. This paper presents the various categories of multimodal system, the techniques – index codes, Gittins index algorithm, used for pattern retrieval from large database & its applications.**

Index Terms— Multibiometric, unimodal, biometric, index codes, index algorithm

I. Introduction

Biometrics refers to metrics related to human characteristics and traits. Biometric identification (or biometric authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are often categorized as physiological versus behavioral characteristics.

Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm print, face recognition, DNA, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.

Some desirable properties of biometric characteristics for good discrimination and reliable recognition performance are as follows:

- *Universality*: Every individual should possess the characteristic.
- *Uniqueness*: The characteristics should be sufficiently distinguishable across individuals comprising the population.
- *Permanence*: The biometric characteristics should be sufficiently invariant over a period of time.
- *Measurability*: It should be possible to acquire the characteristics without causing undue inconvenience. The acquired raw data should be suitable for further processing.

From an application point of view, following properties should also be taken into account.

- *Performance*: The required recognition accuracy in an application should be achievable using the characteristics.
- *Acceptability*: Acceptability refers to the willingness by the subject to present his biometric characteristics.
- *Spoof Resistance*: This refers to how difficult it is to use artifacts (for example, fake fingers) in case of physiological characteristics and mimicry in case of behavioral characteristics.

A number of biometric characteristics exist and are in use in various applications. Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is “optimal.” The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic. A brief introduction to the commonly used biometrics is given below.

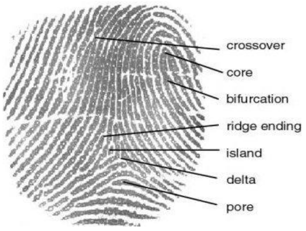


Fig. (a)

- *Fingerprints:*

Fingerprints, as shown in Fig. (a) are unique and consistent over time and hence being used since a long time. A fingerprint is a pattern of ridges and valleys on the surface of a fingertip. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The various kinds of discontinuities in ridges (minutiae) have sufficient discriminatory information to recognize fingerprints. Ridge bifurcation (where the ridge splits) and ridge ending (where the ridge ends) are the important minutiae points. Minutiae-based fingerprint recognition usually represents fingerprint by these two ridge characteristics called as minutiae. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Availability of multiple fingerprints of a person makes fingerprint recognition suitable for use in large-scale identification involving millions of identities. However, the problem with the large scale fingerprint recognition system is

Manuscript received August 19, 2014.

Kshama Dwivedi, pursing ME (Computer Engineering) ARMIET, Asangaon (Mumbai), India

Sachin Singh Thakur, pursuing MTech(Computer Science) T.I.T, Bhopal (M.P.), India

Mayur Shishupal, - pursuing ME (Electronics & Telecommunication) Y.T.I.E.T. Bhivpuri (Mumbai), India

Aarti Bhirud, - pursuing ME (Computer Engineering) Y.T.I.E.T. Bhivpuri (Mumbai), India.

the requirement of huge amount of computational resources, especially in the identification mode.

- *Face:*

Face recognition as shown in Fig (b) is a non-intrusive method and also requires minimum cooperation from the subject. The dimensions, proportions and physical attributes of a person's face are unique. In some application scenario like crowd surveillance, face recognition probably is the only feasible modality to be used. Face recognition can be in a static controlled environment or a dynamic uncontrolled environment. One popular approach to face recognition is based on the location, dimensions and proportions of facial attributes such as eyes, eyebrows, nose, lips, and chin and their spatial relationships. Another approach being widely used is based on the overall analysis of the face image that represents face as a weighted combination of a number of canonical faces.

Face recognition involves two major tasks: i) face location and ii) face recognition. Face location is determining the location of face in the input image. For recognizing the located face, the eigenface approach is one of the very popular methods. The eigenface-based recognition method consists of two stages: i) training stage and ii) operational stage. In the training stage, training set of face images are acquired. The acquired face images are projected into lower dimensional subspace using Principle Component Analysis (PCA). A set of images that best describe the distribution of training images in a lower dimensional face space (the eigenspace) is computed. Then the training facial images are projected into this eigenspace to generate representation of the training images in the eigenspace. In the operational stage, the input face image is projected into the same eigenspace that the training samples were projected into. Then, recognition can be performed by a classifier operating in the eigenspace.

Fig (b)

- *Iris and Retina:*

Fig (c) show the difference between iris and retina scan. Iris is the annular region of the eye regulating the size of the pupil. It is bounded by pupil and sclera (white of the eye) on either side. Iris develops during prenatal period and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. Irises of twins are different as well. Iris based recognition systems provide promising speed and accuracy and support large scale identification operations as well. Contact lenses printed with fake iris can be detected. The hippus movement of the eye can also be used for liveness detection.

The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image acquisition requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect the public acceptability of retinal biometric. Retinal vasculature can reveal some medical conditions, e.g., hypertension, which is another factor deterring the public acceptance of retinalscan-based biometrics.

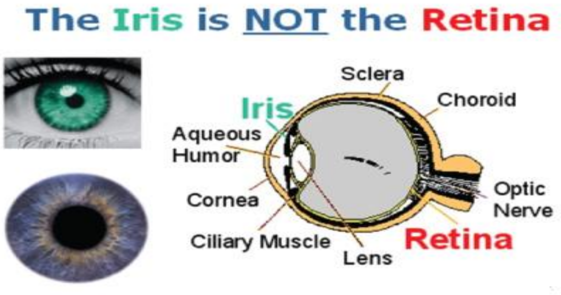


Fig (c)

- *Ear*:

It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. The ear recognition as shown in the Fig (d) approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

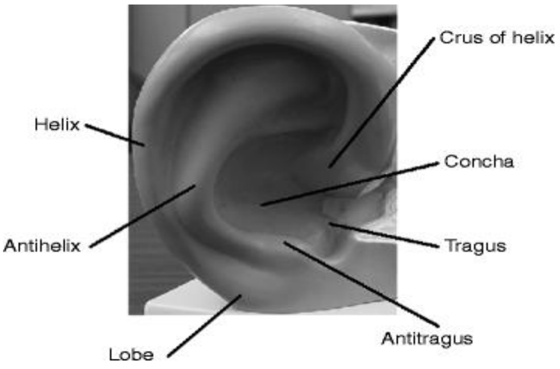


Fig (d)

- *DNA*:

As shown in the Fig (e) Deoxyribonucleic acid (DNA) is the one-dimensional (1–D) ultimate unique code for one's individuality— except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. Three issues limit the utility of this biometrics for other applications: 1) contamination and sensitivity: it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose; 2) automatic real-time recognition issues: the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not geared for on-line noninvasive recognition; and 3) privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g., in hiring practices.

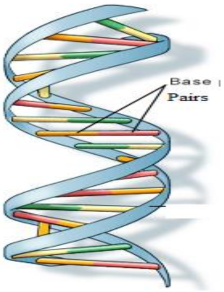


Fig (e)

- *Gait*:

As shown in the Fig (f) gait is the peculiar way one walks and is a complex spatio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications. Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints or brain, or due to inebriety. Acquisition of gait is similar to acquiring a facial picture and, hence, may be an acceptable biometric. Since gait-based systems use the video-sequence footage of a walking person to measure several different movements of each articulate joint, it is input intensive and computationally expensive.

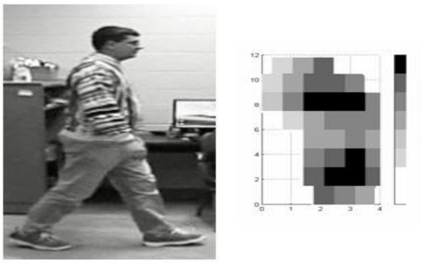


Fig (f)

- *Signature*:

The way a person signs his or her name is known to be a characteristic of that individual, as shown in the Fig (g). Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories.

Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system.

Fig (g)

- *Voice*:

Voice is a combination of physiological and behavioral biometrics. Fig (h) shows how it can be used for identification. The features of an individual’s voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as a common cold), and emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel.

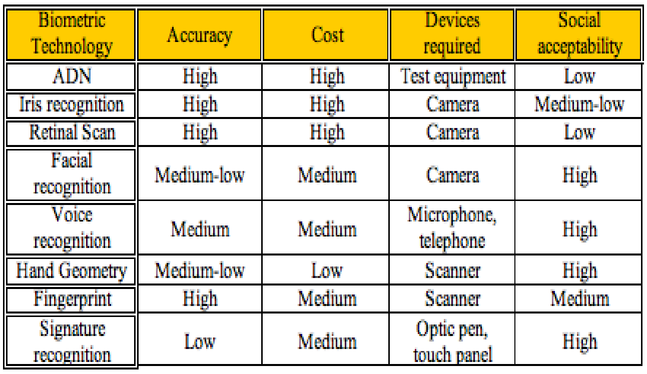
Fig (h)

- *Hand Geometry*:

Hand geometry recognition systems, as shown in the Fig (i) are based on the different measurements such as shape of the hand, size of palm, lengths and widths of the fingers. Hand features are not very distinctive. They are suitable for verification but not for identification. In certain situations such as immigration and border control, biometrics such as fingerprints may not be suitable because they infringe on privacy. In such situations hand geometry can be used for verification as hand geometry is not very distinctive. Hand geometry features may not be invariant during the growth period of children. The size of such recognition systems is large and hence it is difficult to embed the systems in other devices such as laptops.

Fig (i)

A brief comparison of the above biometric techniques based on seven factors is provided in Table-I. The applicability of a specific biometric technique depends heavily on the requirements of the application domain. No single technique can outperform all the others in all operational environments. In this sense, each biometric technique is admissible and there is no optimal biometric characteristic. For example, it is well known that both the fingerprint-based and iris-based techniques are more accurate than the voice-based technique. However, in a tele-banking application, the voice-based technique may be preferred since it can be integrated seamlessly into the existing telephone system.



Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
ADN	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

TABLE-I

II. CATEGORIZATION

The International Committee for Information Technology Standards (INCITS) Technical Committee M1, Biometrics, and researchers have described methods for performing multibiometric fusion. In general, the use of the terms multimodal or multibiometric indicates the presence and use of more than one biometric aspect (modality, sensor, instance and/or algorithm) in some form of combined use for making a specific biometric verification/identification decision. The goal of multi-biometrics is to reduce one or more of the following:

- False accept rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate (FTE)
- Susceptibility to artifacts or mimics

To further the understanding of the distinction among the multi-biometric categories, they are briefly summarized in the following:

Multimodal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example, a system combining face and iris characteristics for biometric recognition would be considered a “multimodal” system regardless of whether face and iris images were captured by different or same imaging devices. It is not required that the various measures be mathematically combined in anyway. For example, a system with fingerprint and face recognition would be considered “multimodal” even if the “OR” rule was being applied, allowing users to be verified using either of the modalities.

Multialgorithmic biometric systems take a single sample from a single sensor and process that sample with two or more different algorithms. The technique could be applied to any modality. Maximum benefit would be derived from algorithms that are based on distinctly different and independent principles.

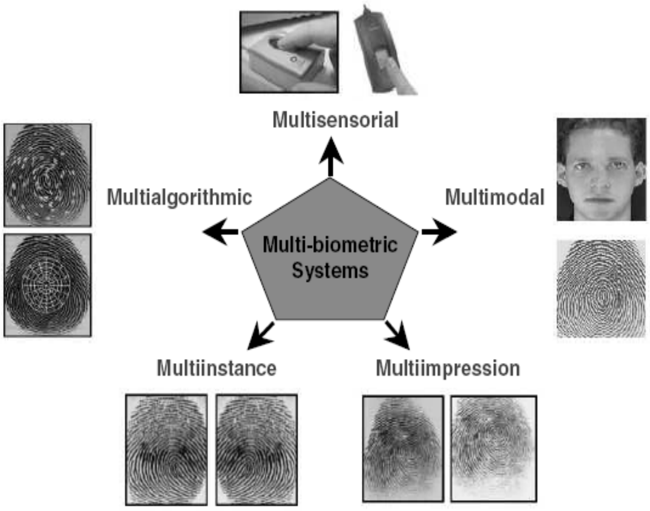


Fig. 1 : Categories of Multibiometric System

Multiinstance biometric systems use one sensor (or possibly multiple sensors) to capture samples of two or more different instances of the same biometric characteristics. For example, systems capturing images from multiple fingers are considered to be multiinstance rather than multimodal. However, systems capturing, for example, sequential frames of facial or iris images are considered to be multi presentation rather than multiinstance. This is whether or not the repeated captured images are combined at the image (feature) level, some other level of combination or a single image is selected as the one best used for pattern matching.

Multisensorial biometric systems sample the same instance of a biometric trait with two or more distinctly different sensors. Processing of the multiple samples can be done with one algorithm or some combination of multiple algorithms. For example, a face recognition application could use both a visible light camera and an infrared camera coupled with specific frequency (or several frequencies) of infrared illumination. For a specific application in an operational environment, there are numerous system design considerations, and trade-offs that must be made among factors such as improved performance (e.g., verification or identification accuracy, system speed and throughput, robustness, and resource requirements), acceptability, circumvention, ease of use, operational cost, environment flexibility and population flexibility. Especially for a large-scale identification system, there are additional system design considerations such as operation and maintenance, reliability, system acquisition cost, life cycle cost and planned system response to identified susceptible means of attacks, all of which will affect the overall deploy ability of the system.

III. RETRIEVAL TECHNIQUES

First Approach :

In a biometric identification system, the identity corresponding to the input data (probe/investigation) is typically determined by comparing it against the templates of all identities in a database (gallery).Exhaustive/in-depth matching against a large number of identities increases the response time of the system and may also reduce the accuracy of identification. One way to reduce the response time is by designing biometric templates that allow for rapid matching. An alternative approach is to limit the number of identities against which matching is performed based on criteria that are fast to evaluate. In this technique the search space is reduced by partitioning the database into several bins. Following such binning, the biometric database will be partitioned such that the templates in each bin are similar and correspond to some natural or statistical class. In case of the traditional 1: N comparisons for identification, the time needed for the system would be to determine the distance between the test template and the N templates in database. Thus the total time needed in such a case could be given as: Q (N). This is achieved by reducing the search space using Gittins index algorithm and it also improves the accuracy of identification.

.

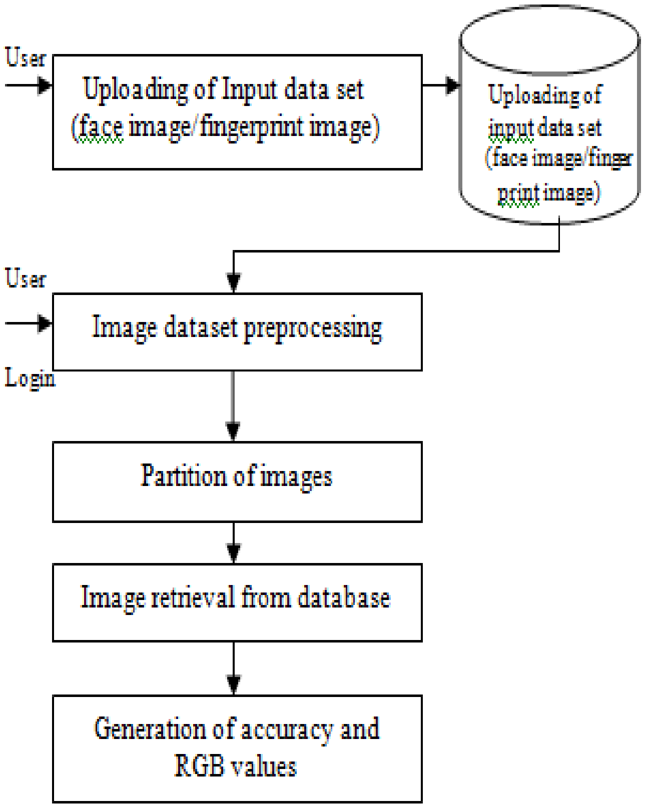

User
Uploading of Input data set
(face image/fingerprint image)
Uploading of input data set (face image/finger print image)
User
Login
Image dataset preprocessing
Partition of images
Image retrieval from database
Generation of accuracy and RGB values

Fig. 2: Architecture Diagram

1. Dataset Pre-processing:
In the dataset preprocessing the images of face and finger print are collected and stored in the database .For face images we use dataset from FERET and the FRGC and fro finger print images we use WVU fingerprint database. There are 1195 subjects with frontal face images in the FERET database. We use only 1010 of these subjects because the images of the remaining 185 subjects could not be processed The WVU fingerprint database contains images of 4 different fingers (left index, left thumb, right index, right thumb) from 270 subjects. We treated the individual fingers as independent "subjects," resulting in a total of 1080 subjects.

2. Generation of Index codes for all the Images:
The index code of an image is the list of its match scores against the reference images. An image is taken and it is matched with the set of reference images already stored in the database. So as compared to the number of reference images the index codes varies the reference images may be viewed as "basis" vectors in the original feature space. If two images ,the input and reference images are similar then their values are expected to be lesser than the threshold ,where the threshold is set before processing ,if the C values are greater than threshold
it is assumed that the two images belongs to different individuals. During identification, the indexing system first computes the index code S of the probe. Then it outputs all enrolled identities whose index codes are within a certain distance from S. The index codes are generated from both face and Fingerprint Images.

3. Input Image Clipping Processing:
Clipping refers to any procedure which identifies the portion of a picture which is either inside or outside a region using any clipping algorithm. The region against which an object is to be clipped is; called clipping window. Clipping is a process of capturing or processing an image where the intensity in a certain area falls outside the minimum and maximum intensity which can be represented. In the input image clipping process, the input image is partitioned into several patches and each patch will search for corresponding matches in database. If any match is found then RGB and color code value is generated for that image.

4. Selecting the reference Image and retrieving the Image**:**
Reference images can be selected from the database itself. They can also be synthetically generated images. While the entire database can be viewed as a candidate pool for selecting reference images, practical considerations dictate the use of a small random subset of images for this purpose.

Second Approach:

The retrieval of a small number of candidate identities from a database based on the probe data is known as database *filtering*. Filtering can be accomplished by using classification or indexing schemes. In a classification scheme, identities in the database are partitioned into several classes. Only the identities belonging to the same class as that of the probe image are retrieved during the search process for further comparison. This approach has two main limitations: 1) it assumes that each identity can be unambiguously assigned to a single class; and 2) the distribution of identities across classes may be uneven resulting in inefficient classification.

In contrast, the goal of an indexing scheme is to assign a unique index value to every identity in the database. However, the index value of the probe image may not be identical to that of the corresponding identity in the database because the process of biometric acquisition and processing is susceptible to noise. Therefore, the retrieval scheme has to employ some type of neighborhood search in the index space. An efficient indexing algorithm retrieves a small number of candidate identities based on similarity measures that can be computed quickly. An important advantage of indexing techniques is that they do not create "boundaries" among the continuously distributed templates.

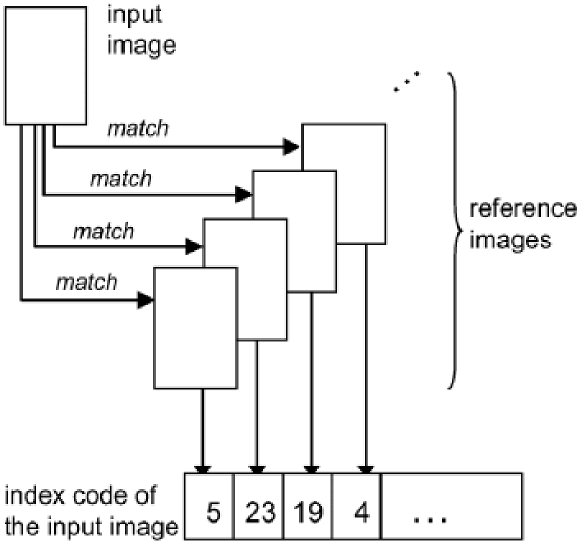


Fig. 3: Generation of an index code. An input image is matched against a set of reference images. The set of resulting match scores constitutes the index code of this input image.

Index Codes For Multimodal Databases

There is an inherent trade-off between the total number of retrieved candidates and the number of *correctly* retrieved candidates. Fusion schemes are often useful for narrowing down the total number of retrieved candidates and/or increasing the number of correctly retrieved candidates. In biometric identification, it is crucial that the correct identity is in the candidate list even if this results in a longer list. We propose two fusion techniques that use the information from multiple modalities in a complementary manner. Index codes are stored separately for each modality thereby making the indexing scheme flexible in including more modalities or excluding a certain modality. The ability to exclude a modality from the indexing process is valuable when prior knowledge indicates that a certain modality is unreliable or when data for a modality are missing. This approach for indexing multimodal databases is shown in Fig. 4.

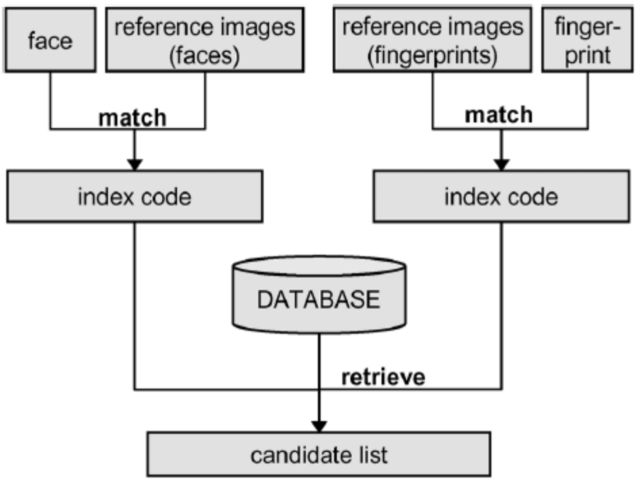


Fig. 4: Indexing two modalities. Two index codes are generated separately, one for each modality. The information from the two modalities is combined during retrieval.

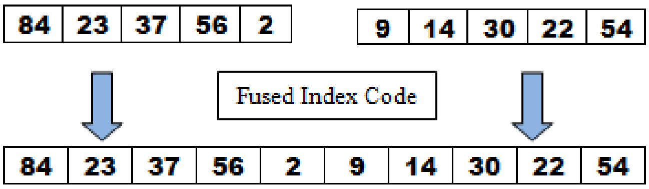


Fig. 5: Fusion by concatenation of index codes

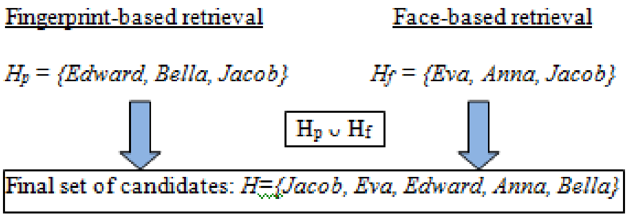

Fingerprint-based retrieval
Face-based retrieval
H_p = {Edward, Bella, Jacob}
H_f = {Eva, Anna, Jacob}
$H_p \cup H_f$
Final set of candidates: H={Jacob, Eva, Edward, Anna, Bella}

Fig. 6: Fusion by union of candidate lists

A. Concatenation of Index Codes

Let $S_x(R^i) = \{s(x^i, r_1^i), s(x^i, r_2^i), \ldots, s(x^i, r_n^i)\}$ be the index code of identity , where i denotes the modality, r_j denotes the jth reference image in this modality, and $s(a, b)$ denotes the match score between a and b. The fusd index codes from different modalities:

$$F_x = \{ s(x^1, r_1^1), \ldots, s(x^1, r_n^1), s(x^2, r_1^2), \ldots, s(x^2, r_n^2)\}.$$

Fig. 5 illustrates this process schematically. Retrieval using the fused index code is performed as for a single modality. This fusion scheme results in longer index codes. Ideally, using longer index codes results in larger variances among them—this is desirable. One weakness of this fusion scheme is that poor indexing performance due to one of the modalities can negatively affect the overall performance of indexing.

B. Union of Candidate Lists

Another fusion mechanism is to combine the lists of candidate identities output by each modality. Let C^i be the set of retrieved identities according to modality. The final set of identities retrieved by the indexing will be $C = U_{i=1}^{k} C^i$ as shown in Fig. 6. This fusion scheme has the potential to increase the chances of finding the right identity in even if the right identity is not located in some of the C^i's. Thus, poor indexing performance of one modality would have a smaller effect on the overall indexing performance. This approach fails only when the right identity is not retrieved by any of the modalities. Intersection of the identities in the candidate lists is another option for indexing multimodal databases but is not discussed in this paper due to its inferior performance.

IV. APPLICATIONS

Applications can be categorized into three main groups:

1) Commercial applications such as computer network login, e-commerce, Internet access, ATMs or credit cards, physical access control, mobile phones, Personal Digital Assistant (PDA)s, medical records management, distance learning, etc.

2) Government applications such as national ID card, driver's license, social security, border control, passport control, welfare-disbursement, etc.

3) Forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, etc.

V. CONCLUSION

This paper overviews and discusses the various scenarios that are possible in multimodal biometric systems using fingerprint, face and iris recognition, the techniques that can be adopted to retrieve the information and improve overall system accuracy.

REFERENCES

[1] A. Ross and A.K. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letter* 24, pp.2115-2125, 2003.
[2] A. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.
[3] ISO/IEC JTC 1/SC 37 Biometrics, *Working Draft Technical Report on Multi-Modal and Other Multi-Biometric Fusion*, August 2005.
[4] S. Prabhakar and A.K. Jain, "Decision-level fusion in fingerprint verification", *Pattern Recognition*, Vol. 35, No. 4, pp. 861-874, 2002.
[5] H. Korves, L. Nadel, B. Ulery, and D. Masi, "Multibiometric Fusion: From Research to Operations", *Sigma*, Mitretek Systems, Summer 2005.
[6] "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability," November 13, 2002.
[7] A. Mhatre, S. Palla, S. Chikkerur, and V. Govindaraju, "Efficient search and retrieval in biometric databases," Biometric Technol.Human Identification II, vol. 5779, no. 1, pp. 265–273, 2005
[8] A. Gyaourova and A. Ross, "A coding scheme for indexing multimodal biometric databases," in Proc. IEEE Computer Society Workshop on Biometrics at the Computer Vision and Pattern Recognition (CVPR) Conf., Miami, FL, Jun. 2009.
[9]http://www.biometric solutions.com/applications/index.php
[10] http://www.intechopen.com/books/recent-application-in-biometrics