IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 07-12
www.iosrjournals.org

Modern Biometric Technologies: Technical Issues and Research Opportunities

Mandeep Singh Walia
(Electronics and Communication Engg, Panjab University SSG Regional Centre, India)

Abstract : *A biometric system is pattern recognition system that recognizes a person by determining the authenticity of a specific characteristic as physiological and/or behavioral possessed by that person. The general definition of a biometric system given above can have a broad interpretation that is not necessarily helpful when considering the nature of modern biometric applications and their uses. Biometric applications have the potential to offer much more robust authentication/identification security than traditional systems. . In fact, the widespread adoption of biometrics solutions has profound implications for how we view the relationship between the individual and the state. However, as with any technology, unique factors and limitations are considered within the context of the application domain. Research into several interrelated areas will bring continued improvement. In this paper, technical and engineering issues are discussed with several opportunities of modern biometric technologies.*

Keywords: *DNA, face, fingerprint, iris, voice*

I. INTRODUCTION

Modern biometric systems can be traced through the evolution of scientific inquiry, empirical evaluation and classification of a given physical or behavioral trait into sub-types. The fundamental computing concepts at the core of modern biometrics include image processing, pattern recognition, statistics, basic signaling and some machine learning models such as knowledge based systems and neural nets. Modern biometric system is the automatic measurement and subsequent recognition of such traits with electronic means. Up until the late 1980's fingerprint technology in the form of AFIS were to dominate the biometric industry with specialized applications in the area of forensic criminology and government security. However, continued in the development of image processing and pattern recognition as Automatic or Machine recognition to distinguish pattern of interest from their background and make suitable decisions about the categories of patterns. Where pattern is quantitative or structural description of an object or some other entity of interest (like speech signal, Intensity image of PCB, DNA, Multi spectral image, Document image, fingerprint image, face image, iris image etc.) [1].

II. TECHNICAL ISSUES

Every biometric system relies on one or more biometric modalities. The choice of modality is a key driver of how the system is architected, how it is presented to the user, and how match vs. non-match decisions are made. Any human physiological or behavioral characteristics can serve for a biometric System as long as it satisfies the Universality (Everyone should have it), Distinctiveness (It should not be the same), Permanence (It should be invariant over a given period of time), Collectability, Performance (It should have accuracy, speed and resource requirements), Acceptability (It must be harmless to users), and Circumvention (it should be robust enough to various fraudulent methods) [2]. The technical issues in terms of performance metrics, accuracy and usability are given below.

2.1. Performance Metrics

Due to different positioning on the acquiring sensor, imperfect imaging conditions, environmental changes, deformations, noise and bad user's interaction with the sensor, it is impossible that two samples of the same biometric characteristic, acquired in different sessions exactly coincide. The following performance metrics are used for recognition systems:

- False accept rate or false match rate (FAR or FMR) – the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.
- False reject rate or false non-match rate (FRR or FNMR) – the probability that the system fails to detects a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

- Relative or Receiver operating characteristic (ROC) – The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- Equal error rate or crossover error rate (EER or CER) – the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.
- Template capacity and scale – With an increase in the size of the database, there is a need for scaling the system to control the false- match error rates. Scaling include multiple hardware units and coarse pattern classification. Hardware which is directly proportional to the database size will be expensive. Coarse pattern classification is happen only when multiple measures are available and efficient indexing algorithms need instead of generic approach applicable for all biometric measures.
- The performance of biometrics in terms of metrics is False Acceptance Rate (FAR) and False Rejection Rate (FRR). The use of such metrics is that the same biometric feature can never generate two identical templates. This is due to environmental factors (humidity and light intensity), inconsistence performance of the hardware, and human aging with variation of posture of the biometric. The challenge is to design a secure biometric system that will never be fooled by spoofed measurements injected into the system which result in compromised identifiers. Biometric system is concerned with privacy as there is fear that widespread use of biometrics will affect on privacy of individual. The use of biometrics occur the fear is that the system might be hazardous to health as using of infrared light to scan retina pattern of eyes.

2.2. Accuracy

The accuracy is affected by sample taken under conditions whether as close or farther during the enrollment process. As in speech recognition, sound of other systems (fan, air conditioning system) turn on while capturing during the enrollment process. In finger scanning, it may fail if pressure of placement of finger is different during the enrollment process. Other factors that fail biometric systems are wearing of glasses, light intensity, and colored contact lenses.

2.3. Usability

An effective biometric should have ease of use, health, privacy and security. The advantage of biometrics over password and token is that user no longer needs to carry with them or remember anything. It would be difficult for biometrics to gain popularity, if it is hard to use. The ease of biometric system can be assessed by trained and enrolled/identification time, maintain and scalability of the system and to protect the health of the user. Availability is important in regard of usability as a system that is not available for service is useless for most of the time, regardless of the ease of use. Convenience is achieved by scarifying certain amount of security. A low threshold value is needed to reduce the number of times of asking users to resubmit samples and it downgrade the system's security.

III. RESEARCH OPPORTUNITIES

In recent years several research agendas for biometric technologies and systems have set important challenges for the field. In recent years biometrics has become a commercially viable technology and will certainly bring about profound changes in our everyday lives as it continues to develop. However, misconceptions of the technical and performance side as well as the social impact of biometric systems, has lead to a distortion of the facts. This section gives the research opportunities to the most common biometric identifiers and typical biometric system.

3.1. Face

Face recognition is considered one of the most non-intrusive of biometric methodologies because we naturally use distinguishing facial characteristics to differentiate between people every day. Our brain has specialized nerve cells responding to specific local features and our visual cortex must combine the different

sources of information into useful patterns. In automatic recognition, extracting meaningful features, representing those features and then performing classification on them. Image encoding can be either localized or global. Local models are based on establishing the relationship between a number of facial features, such as the distance between the eyes, or the distance between each eye and the nose etc. The global model is template-based, such as the eigenface approach [3]. Any human face can be considered a combination of the standard sub-set of these eigenfaces. Each eigenface represents a pattern of evaluation for different facial features and another technique, fisherfaces, is said to be less sensitive to light variation and facial angle [4].

Face recognition an easy task for humans, even one to three day old babies are able to distinguish between known faces [5]. There are several questions arising for facial recognition are to analyze image and how brain encode it, inner features or outer features for successful face recognition. Ongoing opportunities for facial recognition are segmentation—distinguishing facial features from surrounding information. Another significant challenge for it is invariant representation—that is, finding a representation that is robust and persistent even when there are changes in pose, expression, illumination, and imaging distance.

For image capture, standard optical scanners can be used as still photos and live capture. Certain newer technologies acquire a 3D image of the face using stereo, structured light or phase-based ranging and near infrared can be used to supplement face detection in poor lighting conditions.

Due to non-availability of sufficient number of training samples, uncontrolled or variance in the conditions, the matcher may not correctly model the invariance relationship resulting in poor matching accuracy.

3.2. Fingerprint

Fingerprint-based identification is the oldest biometric system in terms of successful practical application. Fingerprints are most widely recognized biometric for criminal justice application, border security and identity proofing. The invariant and immutable aspects of a fingerprint supposedly lie in the patterns of ridges and furrows, as well as the ridge characteristics occurring at either a ridge bifurcation or a ridge ending – the so called minutiae points. Three major techniques are identified in the literature for fingerprint representation and matching, they include – image or correlation techniques, minutiae based methods and hybrid or ridge feature based approaches.

The issues related to the development of mobile capture devices and scanner issues include artifact noise and feature extraction errors. For representation limitation, the ideal representation should be designed to retain invariance in the measurements that sensed. The poor quality images that cannot process with traditional fingerprint recognition system thus conventional representations are limiting the discrimination among the images.

When capturing a fingerprint image, consideration must be given to the image resolution quality provided by the scanner. Varying image quality leads to a variation in the range and type of features available for analysis. Another Unique consideration for fingerprint biometrics is that the user, when enrolling or authenticating, must touch the scanning device. Artifacts may gather on the platen in the form of smudges and dirt from natural skin oil or the platen may become scratched as a result of contact. Therefore, scanner quality, (pixel intensity), and usage combine to create a large variability in different impressions of the same finger. In representation terms this is referred to as a high intra-class variation, i.e. images of the same finger may look different. Conversely, a low inter-class variation leads to images from different fingers looking quite similar. The ideal is to create a low intra-class variation, by finding a measurable feature space that allows clustering of same finger images, while images for different fingers occupy a different area of the space, (high inter-class variation).

Therefore, the implication for ideal matching is that the similarity between two representations of the same finger should be large, or alternately, the distance in the feature space between the images should be small. In other words the properties of the representation methodology should be, as much as possible, invariant to the key problems of intra-class variation. Ridge feature-based methods are a hybrid of both local and global representation techniques in an attempt to overcome the main drawbacks of each. Local minutiae extraction may be impossible for low quality fingerprint images. Other features of the ridge pattern such as local orientation, frequency, and texture information can be extracted more reliably than minutiae. Understanding particular modalities and how best to use the modalities is critical to overall system effectiveness. Specific challenges with respect to fingerprints include reducing the failure to enroll (FTE) and failure to acquire (FTA) rate, perhaps through the design of new sensors, artifact detection, image quality definition and enhancement, and high-resolution fingerprint matching.

3.3. Iris

Iris patterns are very complex and the combination of complexity with randomness confers mathematical uniqueness to a given iris pattern. The iris is differentiated by several characteristics including ligaments, furrows, ridges, crypts, rings, corona, and freckles. The idea of using the iris as a biometric is over 100 years old. Daugman was Successful and in 1994, Dr. John Daugman of Cambridge University's computer laboratory developed the key algorithms for image capture, feature extraction and matching [6] and gives a comprehensive account of the technical and performance aspects of his algorithms.

The key problems during feature extraction are occluded iris, shadow on iris and light reflection as shown in Fig.1. Other challenges are detecting the pupil, (which can vary up to 15% from a central position in the eye) and removing noise created by eye-glasses or light reflection on the cornea as well as parts of the iris obscured by the eyelashes or drooping of the eyelid. This is achieved by using edge detection to create zones of texture across the iris by differentiating between the sclera, white of the eye, on the outer zone and the varying dilation of the pupil on the inner zone.

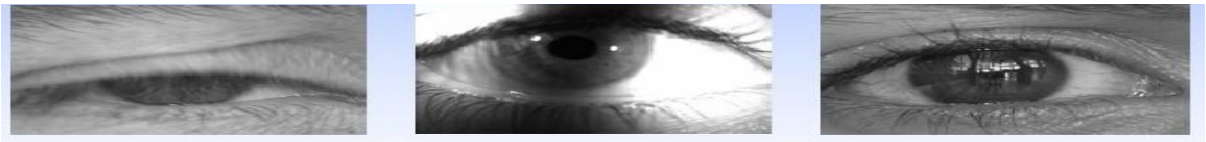

Fig.1. occluded iris, shadow on iris and light reflection

The primary reasons that underlying imperfect accuracy performance of a biometric systems are information limitation, representation limitation, and invariance limitation [7]. The pattern samples with invariant and distinctive information may be limited due to intrinsic signal capacity of the biometric identifier. The information limitation may be due to unsupervised controlled signal acquisition. Iris recognition systems present R&D opportunities in the following areas: sensors; optimization of the illumination spectrum; reducing FTE and FTA rates; capturing and recognizing the iris at greater distances and with movement of the subject; and reducing the size of the hardware.

To further the advances made in iris recognition over the past decade, researchers must solve issues such as capturing eye images of sufficient quality in less than ideal conditions and accurately localizing the iris's spatial extent in poor-quality images. However, the promise of iris recognition —borne out by the complexity of the patterns and their assumed stability—is compelling motivation to solve these problems and facilitate a broader use of iris recognition systems. A method that upgrades the traditional iris recognition system to work on nonideal situations takes into consideration not only the effect of image quality but also the segmentation accuracy.

The video-based image-processing techniques are quickly identified and eliminate the bad quality images from iris videos for further processing**.** The effects of defocus blur, motion blur, off-angle view, occlusion, specularities, lighting, and pixel counts on image quality are considered [8]. Estimated individual factors are combined into an overall quality metric using a Dempster–Shafer approach. It is shown that the quality metric can predict recognition performance reasonably well. It is also noted that the computation of the quality metric requires an initial segmentation, and that "failed localization/segmentation will result in inaccurate quality scores.

To remove the irregularities present in iris images, appropriate global enhancement functions are applied on the input iris image. While these algorithms enhance regions of the image with poor quality, they also change the characteristics of the image that are of acceptable or high quality. Moreover, the poor quality of an image may be due to multiple irregularities such as excessive noise, poor illumination, or motion artifacts introduced during image capture.

The challenge in enhancing such images is to locally segment the affected regions from the image and apply appropriate enhancement algorithms. So far, there have been many different approaches for iris image segmentation. However, none of these iris segmentation methods can achieve 100% accuracy. To improve the iris recognition accuracy, it is desirable to have an iris segmentation evaluation system. The reduction in complexity by encoding and efficiency of the matching algorithms will also become more important as recognition application is deployed for large populations. Another area that has not received much attention yet is how to combine multiple images to improve performance and to see how recognition could be improved for people wearing glasses.

3.4. Voice

Voice is an acceptable biometric for many and in fact is the only possible biometric for most audio-technologies. It is important to note that there is a distinction made between voice verification or speaker recognition, (i.e. identifying a specific speaker) and speech recognition, (i.e. identifying what is being said). Voice, like other biometrics, cannot be forgotten or misplaced, unlike knowledge-based (e.g., password) or possession-based (e.g., key) access control methods. Old method of identification of speaker was identification through spectrograms. But this method had lot of problems and difficulties. To overcome the shortcomings of previous technique, the idea of automatic speaker identification is suggested. In this features are first extracted from speech samples and then after modeling, the samples are stored in a speaker database as shown in Fig.2. For speaker identification, when matching required, the features are again extracted from speech samples and are compare with stored database. A decision is taken on the basis of this match to accept or reject the sample.

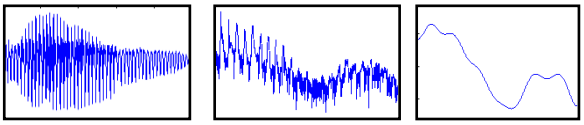

Fig.2. speech signal, spectrum and smoothed spectrum

Generally, speaker recognition systems must first convert captured analogue speech signals to digital and further process them using spectral analysis principles. Typically, Fourier transforms can be used to derive coefficients for complex audio wave functions which in turn can be used to isolate the ceptstral feature vector for representing the human voice. Research into speaker recognition goes back over forty years and relies on both behavioral and physical traits. Physical traits include such properties as the size and shape of the vocal chords, vocal tract, palate and learned behaviors include style of speech, voice pitch and timbre. The fact that behavioral as well as physical traits combine in resulting speaker system templates or "voice prints", leads to the method being classified as a behavioral biometric in general. The ubiquity of acoustic technology such as telephony makes speaker recognition an attractive security option. This is because it is often possible to take advantage of existing audio hardware when deploying such systems.

Speaker Identification can be improved by speaker separation, normalizing channels, and using higher level information. In addition robustness and persistence are needed would all offer opportunities to improve voice recognition. In addition, robustness and persistence are needed in the face of language and behavioral changes and the limited number of speech samples Real time speaker identification having a lot of scope for work in future. For implementation of speaker identification DSP processor [9] can be used.

3.5. DNA

DNA is currently used to perform forensic identifications. Technological advancement for the development is portable rapid DNA machines. This machine can identify border agents to confirm identification individually and/or family relationships and provide a new tool for rapid identification. This can be significant advancement in the use of biometrics for criminals and antiterrorism applications.

3.6. Technological Opportunities of Typical Biometric Recognition System

A biometric recognition system is essentially a system that operates by acquiring data from an individual and then does preprocessing, segmentation, extracting the features set and comparing the feature set against the template set in the database. The challenges and opportunities of biometric system are discussed below:

- Sensors – The cost of sensor hardware; improving the signal-to-noise ratio, the ease of use and affordability, and the repeatability of measures; and extending life expectancy.
- Segmentation – Improving the reliability of identifying a region of interest when the user presents his or her biometric characteristics to the system—for example, locating the face(s) in an image or separating speech signal from ambient noise.
- Invariant representation – Finding better ways to extract invariant representation (features) from the inherently varying biometric signal—that is, what kind of digital representation should be used for a face (or fingerprint or other feature) such that the trait can be recognized despite changes in pose, illumination, expression, aging, and so on.

- Robust matching – Improving the performance of the matching algorithm in the presence of imperfect segmentation, noisy features, and inherent signal variance.
- Privacy– Advance technology to enable solutions to benefit from unique advantages while limiting the risks to privacy.
- Testing– To provide the focus to continue the advances of previous challenges period.

IV. CONCLUSION

The biometric is not a fully solved problem and accuracy of current biometrics systems are not perfect while reliable personal recognition is critical to many business processes. New traits and sensors, salient representation, robust matching, multi biometrics systems, and soft biometrics are new research directions. The limitations of biometrics systems are lack of uniqueness in biometric trait, recognition error, administrative / insider attack, non secure infrastructure and security (template, channel and software security). Tradeoff between security and privacy might be necessary. Technical and engineering areas from sustained research are discussed and investigated for future scope.

REFERENCES

[1] A.K. Jain, R.P.W. Duin, and J. Mao, Statistical pattern recognition: A review, IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(1), 2000, 4-37.
[2] A.K. Jain, A. Ross, and S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for video Technology, 14(1), 2004, 4-20.
[3] M. Turk, and A. Pentland, Eigenfaces for recognition, Journal of Cognetive Nueroscience, 3, 1991, 71-86.
[4] P.N. Belhumeur, J.Hespanha, and D. Knegman, Eigenfaces vs Fisherfaces: Recognition using Class Specific Linear Projection, IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7), 1997, 711-720.
[5] T. Chiara, M.C. Viola, and I. Leo, New borns face recognition: Role of inner and outer facial features, Child Development, 77(2), 2006, 297-311.
[6] J. Daugman, High confidence visual recognition of persons by a test of statistical independence, IEEE Transactions on Pattern analysis and Machine Intelligence, 15(11), 1993, 1148-1161.
[7] Y. Du, C. Belcher, Z. Zhou, and R. Ives, Feature correlation evaluation approach for iris feature quality measure, Elsevier, Signal Processing, 90, 2010.
[8] Z. Zhou, Y. Du, and C. Belcher, Transforming traditional iris recognition systems to work in nonideal situations, IEEE Transactions on Industrial Electronics, 56(8), 2009.
[9] E. Lupu, P. G. Pop, and M. Patras, Low complexity speaker recognition system developed on the DSP processor, Proc. 9th Conference Speech and Computer, St. Petersburg, 2004, 20-22.