Biometrics: The Science of Human Recognition –Part I

Ravindrapal M Joshi
M.B.Patel Science College
Anand-388 001, Gujarat

***Abstract*-A large number of physical systems require authentic and reliable personal recognition schemes to determine and confirm the identification of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include organizations in financialservices, health care, e-commerce, telecommunication and government welfaredisbursements, credit card transactions, cellular phone calls and ATM withdrawals.In this paper, we give a brief overview of the field of biometrics and summarize the performance evaluation of such systems.**

***Index terms*–**
Biometrics,identification,recognition, fingerprint performance evaluation

1. INTRODUCTION

The increasing demand for reliable human identification in large-scale government and civil applications has boosted interest in the controlled, scientific testing and evaluation of biometric systems. Just a few years ago, both the scientific community and commercial organizations were reporting performance results based on self-collected databases and ad hoc testing protocols, thus leading to incomparable and often meaningless results [1, 2].

Measurement of physical features such as height, eye color, scars etc, as a method of personal identity is known to date back to the ancient Egyptians Archaeological evidence of fingerprints being used to at least associate a person with some event or transaction is also said to date back to ancient China, Babylonia and Assyria. But it was not until the end of the 19th century that the study of biometrics entered the realm of crime detection. Alphonse Bertillon, a French police clerk and anthropologist, pioneered a method of recording multiple body (anthropometric) measurement for criminal identification purpose. Known as 'Bertillonage' it was adopted by many police authorities worldwide during the 1890s, but soon became obsolete once it was recognized that people could indeed share the same physical measurement[3].

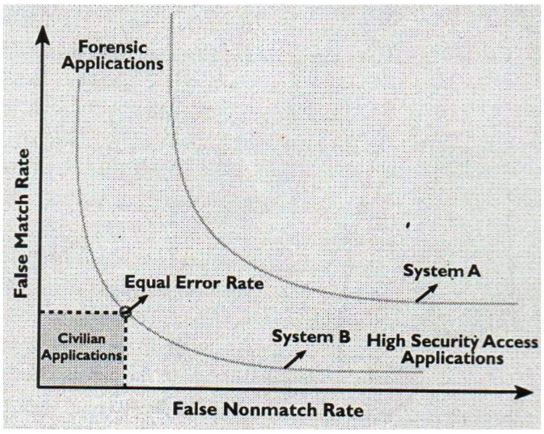
The term ‘biometrics’ is derived from the Greek words bio (life) and metric (to measure).For our use, biometrics refers to technologies for measuring and analyzing a person’s physiological or behavioral characteristics. These characteristics are unique to individuals hence can be used to verify or identify a person.

2.PERFORMANCE EVALUTION

Measuring the performance of biometric identification system is a challenging research topic [4]. The overall performance of biometric system is assessed in terms of its accuracy, speed, and storage. Several other factors like cost and ease-of-use, also affect efficacy. Biometric systems are not perfect, and will sometimes mistakenly accept an impostor as a valid individual (a false match) or conversely, reject a valid individual (a false non-match). The probability of committing these two types of errors are termed false non-match rate(FNR) and false match rate(FMR) ; the magnitudes of these errors depends upon how liberally or conservatively the biometric system operates. Figure 1 shows the trade-off between a system’s FMR and FNR at different operating points; it’s called the” Receiver Operating Characteristics (ROC) “ and is a comprehensive measure of the system accuracy in a given test environment.

High-security access applications, where concern about break-in is great, operate at a small FMR. Forensic applications, where the desire to catch a criminal outweighs the inconvenience of examining a large number of falsely accused individuals, operate their matcher at a high FMR. Civilian applications attempt to operate their matchers at the operating points with both a low FNR and a low FMR. The error rate of the system at an operating point where FMR equals FNR is called the equal error rate (EER)which may often be used as a terse descriptor of system accuracy. Accuracy performance of a biometrics system is consideredacceptable if the risk (benefits) associated with errors in the decision-making at a given operating point on ROC for the given test environment are acceptable. Similarly, accuracy of a biometrics-based identification is unacceptable/poor if risks (benefits) associated with errors related to any operating point on the ROC for a given test environment are unacceptable (insufficient).

Fig.1 Receiver Operating Characteristics (ROC) of a system illustrates false non-match rate (FNR) and false match rate (FMR) of a matcher at all operating points. Each point on a ROC defines FNR and FMR for a given matcher, operating a particular matching score threshold. A smaller FNR (that is, a more tolerant system) usually leads to a larger FMR while a smaller FMR(a less tolerant system)usually implies a larger FNR.Note that System A is consistently inferior to System B in accuracy performance.



The following performance indicators can be measured for fingerprint identification:

- Genuine and impostor score histograms,
- Maximum memory allocated for comparison and forenrollment,
- Failure-to-Compare Rate and Failure-to-Enroll Rate, Zero FMR and ZeroFNMR, Equal Error Rate(EER),FMR100,FMR1000,
- False Match Rate(FMR) and False Non-Match Rate(FNMR) graphs and Decision Error Tradeoff(DET) graph,
- Average and maximum template size, and
- Average comparison time and average enrollment time.

Formal definitions of FMR(False Match Rate),FNMR(False Non-Match Rate),and Equal Error Rate(EER) are given in [1].Note that, in single-attempt, positive recognition applications,FMR(False Match Rate) and FNMR(False Non-Match Rate) are often referred to as FAR(False Acceptance Rate) and FRR(False Rejection Rate),respectively. ZeroFMR is given as the lowest FNMR at which no False Matches occur and ZeroFNMR is the lowest FMR at which no False Non-Matches occur.

FMR10 and FMR1000 are the values of FNMR for FMR=1/100 and 1/1000, respectively. These measures are useful to characterize the accuracy of fingerprint-based systems, which are often operated far from the EER point using thresholds which reduce FMR at the cost of higher FNMR.

FVC2004 introduces indicators measuring the amount of memory required by the algorithms and template sizes. Table 1 summarizes the performance indicators reported in FVC2004 and compares them with those reported in the previous two competitions.

Table 1
Performance Indicators Measured in the Three FVC Competitions

Performance Indicator	**FVC 2000**	**FVC 2002**	**FVC 2004**
Genuine and impostor score histograms	✓	✓	✓
FMR and FNMR graph	✓	✓	✓
DET graph	✓	✓	✓
Failure To Enroll Rate	✓	✓	✓
Failure to Compare Rate	✓	✓	✓
Equal Error Rate (EER)	✓	✓	✓
FMR 100		✓	✓
FMR 1000		✓	✓
Zero FMR	✓	✓	✓
Zero FNMR	✓	✓	✓
Average match time	✓	✓	✓
Average enroll time	✓	✓	✓
Maximum memory allocated for enrollment			✓
Maximum memory allocated for comparison			✓
Average template size			✓
Maximum template size			✓

Taxonomy of offline tests with the following classification (Fig. 2) is described as follows

- In-house-self-defined test: The database is internally collected and the testing protocol is self-defined. Generally, the database is not publicly released, perhaps because of human-subject privacy concerns, and the protocols are not completely explained. As a consequence, results may not be comparable across such tests or reproducible by third party.

- In-house-existing benchmark: The test is performed over a publicly available database, according to an existing protocol, Results are comparable with others obtained using the same protocol on the same number of times to improve performance over the final test set, Examples of recent biometric evolution of this type are [5]database. Besides the trustworthiness problem, themain drawback is the risk of over fitting the data-that is, tuning the parameters of thealgorithms to match only the data specific to this test. In fact, even if the protocol defines disjoint training, validation and test sets, the entire evaluation (including learning) might be repeated a number of times to improve performance over the final test set. Example of recent biometric evaluation of this type is described by J.Matasetal. [5]

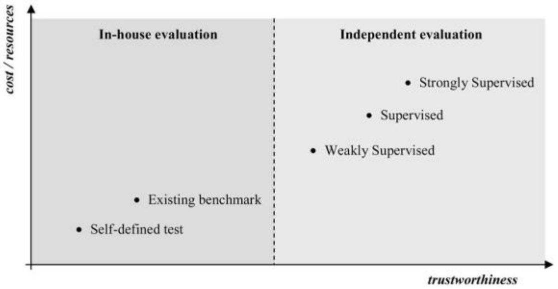


Fig. 2. Classification of offline biometric evaluations.

- Independent-weakly supervised: The database is sequestered and is made available just before the beginning of the test. Samples are unlabeled (the filename does not carry information about the sample's owner identity).The test is executed at the testee's site and must be concluded within given time constraints. Results are determined by the evaluator from the comparison scores obtained by the testee during the test. The main criticism against this kind of evaluation is that it cannot prevent human intervention: visual inspection of the samples, result editing, etc., could, in principle, be carried out with sufficient resources. Example of recent biometric evaluations of this type is given by P.J.Phillips [6].

- Independent-supervised: This approach is very similar to the independent weakly supervised evaluation but, here, the test is executed at the evaluator's site on the testee's hardware. The evaluator can better control the evaluation, but: 1) there is no way to compare computational efficiency (i.e., different hardware systems can be used), 2) some interesting statistics (e.g., template size, memory usage cannot be obtained, and 3) there is no way to prevent score normalization and template consolidation (i.e., techniques where information from previous comparisons are unfairly exploited to increase the accuracy in successive comparisons). Example of recent biometric evaluations of this type is described by P.J.Phillips [7].

- Independent-strongly supervised: Data are sequestered and not released before the conclusion of the test. Software components compliantto a given input/output protocol are tested at the evaluator's site on the evaluator's hardware. The tested algorithm is executed in a totally-controlled environment, where all input/output operations are strictly monitored. The main drawbacks are the large amount of time and resources necessary for the organization of such events. Exampleof recent biometric evaluations of this type is explained by Y.Dit-yen et al. [8] and the FVC2004 evaluation discussed in this paper.

3. CONCLUSION

Biometrics refers to automatic identification of a person based on his or her physiological or behavioral characteristics. It provides a better solution for the increased security requirements of our information society.

Performance evaluation is important for all pattern recognition applications and particularly so for biometrics, which is receiving widespread international attention for citizen identify verification and identification in large-scale applications. Unambiguously and reliably assessing the current state of the technology is mandatory for understanding its limitations and addressing future research requirements.

REFERENCES

[1] Maio D., Maltoni D., Cappelli R., Wayman J.L., and Jain A.K., "FVC2000: Fingerprint Verification Competition," IEEE Trans.Pattern Analysis Machine Intelligence, Vol 24, no. 3, pp. 402-412, Mar 202.

[2] Maio D., Maltoni D., Cappelli R., Wayman J.L., and Jain A.K., "FVC2002: Second Fingerprint Verification Competition," Proc. 16th Int'l Conf. Pattern Reorganization, Vol 3,pp. 811-814, Aug. 2002.

[3] Biometric Consortium homepage www.biometric.org

[4] Wayman, J.L., Error Rate Equations for the General Biometric system. IEEE Robotics & Automation 6.9 (Jan, 1999), 35-48.

[5] Matasetal J., "Comparison of Face Verification Results on the XM2VTS Database,"Proc.15thInt'l Conf.Pattern Recognition, vol.4, pp.858-863, Sept.2000.

[6] Phillips P.J., Moon H., Rizvi S.A .andRaussP.J., "The FERET Evaluation Methodology for Face-Recognition Algorithms," IEEE Tras. Pattern Analysis and Machine Intelligence, Vol 22,no. 10 pp.1090-1104, Oct-2000

[7] Phillips P.J., Grother P.,Micheals R.J., Blackburn,D.M.,TabassiE. and Bone J.M., "Facial Recognition Vendor Test 2002 Evaluation Report,"http://www/frvt.org/FRVT2002 , Mar.2003.

[8] Dit-yenY. et al., "SVC2004: First International Signature Verification Completion," Proc., Int'l Conf. Biometric Authentication, pp.16-22, July. 2004.

Author's Profile

Dr. Ravindrapal M. Joshi received the **Ph.D.** degree in Physics from Sardar Patel University, VallabhVidyanagar,Gujarat in 1990. Currently he is working as an Assistant Professor in M.B. Patel Science College, Anand, Gujarat. He has published seven Research Papers. His research interest includes crystal Growth, Fabrication and Characterization of PEC Solar Cells, Instrumentation, Power Electronics, etc.