UDC 004.056.2+57.087.1

Student O. Kredentser
State University”National mining university”

PERFORMANCE MEASURES OF BIOMETRICS SYSTEMS

The objective of this report is to review existing performance measures of biometrics systems .It also contains the definition on biometrics system as a whole.

Nowadays biometrics system became most safe and fast developed method of information protection. The term “Biometrics” is used alternatively to describe two different aspects of the technology: characteristics and process. Biometrics as characteristics refers to measurable biological or behavioral aspects of the person that can be used for automated recognition. As process it refers to automated methods of recognizing an individual based on measurable biological and behavioral characteristics. A typical biometric system is comprised of five integrated components: a sensor (observes characteristics and converts the observations into data that can be stored in electronic form), signal processing algorithms (that perform quality control activities on the collected data and develop biometric template), a data storage component (manages all of the data collected, including data from the initial and all future collections and processing), a matching algorithm (compares the new biometric template to one or more templates that may already be stored), a decision process (uses the results from the matching component to make a system-level decision).

Performance measures of each biometrics system depend on several parameters:

1. Decision error rates. Biometric performance has traditionally been stated in terms of the decision error rates, viz., “false accept rate” and “false reject rate”. False accept rate is the expected proportion of transactions with wrongful claims of identity (in a positive ID system) or non-identity (in a negative ID system) that are incorrectly confirmed. A false acceptance is often referred to in the mathematical literature as a “Type II” error. Note that “acceptance” always refers to the claim of the user. False reject rate: the expected proportion of transactions with truthful claims of identity (in a positive ID system) or non-identity (in a negative ID

system) that are incorrectly denied. A false rejection is often referred to in the mathematical literature as a “Type I” error. Decision errors are due to matching errors or image acquisition errors. How these fundamental errors combine to form decision errors depends on (a) whether one-to-one or one-to-many matching is required; (b) whether there is a positive or negative claim of identity; and (c) the decision policy, e.g. whether the system allows multiple attempts.

2. Matching errors:

– False match rate (FMR, “false positive”): the expected probability that a sample will be falsely declared to match a single randomly-selected “non-self” template;

– Non-self: Genetically different. It has been noted in the literature that comparison of genetically identical biometric characteristics yields different score distributions than comparison of genetically different characteristics, so they should not be considered in computing the false match rate;

– False non-match rate (FNMR, “false negative”): the expected probability that a sample will be falsely declared not to match a template of the same measure from the same user supplying the sample.

The Difference between decision errors and matching errors is that false match/non-match rates are calculated over the number of comparisons, but false accept/reject rates are calculated over transactions and refer to the acceptance or rejection of the stated hypothesis, whether positive or negative. Further, false accept/reject rates include failure-to-acquire rates. In a positive identification system allowing a maximum of three attempts to be matched to an enrolled template, a false rejection will result with any combination of failures-to-acquire and false non-matches over three attempts. A false acceptance will result if an image is acquired and falsely matched to an enrolled image on any of three attempts. In a negative identification system, a user’s claim not to be enrolled in the system will be falsely rejected if an image is acquired and then falsely matched to one or more enrolled templates.

3. Image acquisition errors:

– Failure to enroll rate: The “failure to enroll” rate is the expected proportion of the population for whom the system is unable to generate repeatable templates. This will include those unable to present the required biometric feature, those unable to produce an image of sufficient quality at enrolment, and those who cannot reliably match their template in attempts to confirm the enrolment is usable. The failure to enroll rate will depend on the enrolment policy;

– Failure to acquire rate: The “failure to acquire” rate is defined as the expected proportion of transactions for which the system is unable to capture or locate an image or signal of sufficient quality. The failure to acquire rate may depend on adjustable thresholds for image or signal quality.

4. Binning algorithm performance:

– Penetration rate: The penetration rate is defined as the expected proportion of the template data to be searched over all input samples under the rule that the search proceeds through the entire partition regardless of whether a match is found. Lower penetration rates indicate fewer searches and, hence, are desirable;

– Binning error rate: A binning error occurs if the enrolment template and a subsequent sample from the same biometric feature on the same user are placed in different partitions. In general, the more partitioning of the database that occurs the lower the penetration rate, but the greater the probability of a binning error.

There are also environmental factors that can affect performance: population demographics, user physiology, user behavior, environment influences, etc.

List of References:

1. http://www.enisa.europa.eu – Europe Network and Information security agency;

2. http://www.biometrics.org – The Biometric Consortium portal.

3. ISSN 1471-0005 – Best Practices in Testing and Reporting Performance Of Biometric Devices.