Appendix A
Evaluation of multibiometric systems

A.1 Biometric system evaluation

Evaluation of a complete biometric system is a complex and challenging task that requires experts from a variety of fields, including statistics, computer science, engineering, business, psychology and law enforcement. In order to gain a thorough understanding of the performance of a biometric system, one must address the following questions.

1. What is the error rate of the biometric system in a given application? (matching or technical performance)
2. What is the reliability, availability and maintainability of the system? (engineering performance)
3. What are the vulnerabilities of the biometric system? What level of security does the biometric system provide to the application in which it is embedded? (security of the biometric system)
4. What is the user acceptability of the system? How does the system address human factor issues like habituation and privacy concerns? (user concerns)
5. What is the cost and throughput of the biometric system and what tangible benefits can be derived from its deployment? (return on investment)

In order to fully evaluate a biometric system, one must also consider the existing security solutions in the application domain where the biometric system will be embedded. No existing biometric evaluation framework addresses all the above questions in a systematic manner. In this appendix, we focus only on the matching performance of a biometric system.

Phillips et al., 2000a have proposed a general framework for evaluating the matching performance of a biometric system. Ideally, the evaluation requires an independent third party to design, administer and analyze the test. Phillips et al., 2000a divide the matching performance evaluation of a biometric system into three stages:

1. Technology evaluation: Technology evaluation compares competing algorithms from a single technology on a standardized database. The Fingerprint Verification Competitions (FVC) (Malo et al., 2004), the Fingerprint Vendor Technology Evaluation (FpVTE) (Wilson et al., 2004), the Face Recognition Vendor Tests (FRVT) (Phillips et al., 2003), the Face Recognition Technology (FERET) program (Phillips et al., 2000b) and the NIST Speaker
Recognition Evaluations (SRE) (Przybocki and Martin, 2004) are examples of biometric technology evaluations. Since the database is fixed, the technology evaluation results are repeatable. However, characteristics of the database such as data collection environment, sample population and user habituation will affect the performance of the algorithms. Hence, care must be taken to ensure that the database is neither too hard nor too easy. If the database is too easy (i.e., it includes only good quality biometric samples with small intra-class variations), the error rates will be close to zero and it will be very difficult to distinguish between the competing systems. On the other hand, if the database is too challenging (i.e., it includes only poor quality biometric samples with large intra-class variations), the evaluation may be beyond the capabilities of existing technologies, thereby rendering the evaluation useless. Ideally, a database should include samples that are representative of the population and it must allow us to distinguish between the performance of competing algorithms and determine their strengths and limitations.

2 **Scenario evaluation:** In scenario evaluation, the testing of the prototype biometric systems is carried out in an environment that closely resembles the real-world application. Since each system will acquire its own biometric data, care must be taken to ensure uniformity in the environmental conditions and sample population across the different prototype systems.

3 **Operational evaluation:** Operational evaluation is used to ascertain the performance of a complete biometric system in a specific application environment with a specific target population.

Mansfield and Wayman, 2002 identify the best practices to be followed when evaluating the technical performance of a biometric system. They make recommendations on a number of testing issues, including size of the test, volunteer selection, factors that may affect the performance of a biometric system, data collection methodology, estimation of the performance metrics, estimating the uncertainty of performance metrics and reporting the performance results. They also note that since their recommendations are general in nature, it may not be possible to follow them completely in any practical biometric system evaluation. A sound evaluation of the technical performance of a biometric system must follow the best practices recommended by Mansfield and Wayman, 2002 as closely as possible and clearly explain any deviations from these recommendations that may be necessary.

A.2 **Issues in multibiometric system evaluation**

Evaluation of the matching performance of a multibiometric system is similar to the evaluation of a unibiometric system except for a few issues that are unique to a multibiometric system. One of the main differences between the evaluation of unimodal and multimodal biometric systems is the nature of the database used. The performance metrics of a biometric system such as accuracy, throughput, and scalability can be estimated with a high degree of confidence only when the system is tested on a large representative database. For example, face (Phillips et al., 2003) and fingerprint (Wilson et al., 2004) recognition systems have been evaluated on large databases (containing samples from more than 25,000 individuals) obtained from a diverse population under a variety of environmental conditions. In contrast, current multimodal systems have been tested only on small databases containing fewer than 1,000 individuals. This is mainly due to the absence of legacy multimodal databases and the cost and effort involved in collecting a large multimodal biometric database.

Multimodal biometric databases can be either true or virtual. In a true multimodal database (e.g., XM2VTS database (Messer et al., 1999)), different biometric cues are collected from the same individual. Virtual multimodal databases contain records which are created by consistently pairing a user from one unimodal database (e.g., face) with a user from another database (e.g.,
The creation of virtual users is based on the assumption that different biometric traits of the same person are independent. While this assumption of independence of the various modalities has not been thoroughly investigated, large virtual multimodal databases are easy to construct assuming that large unimodal databases are available. Indovina et al., 2003 attempt to validate the use of virtual subjects by randomly creating 1,000 sets of virtual users with face and fingerprint modalities. The performance of the multimodal biometric system for the 1,000 virtual user sets is shown in Figure A.1, which indicates that the variation in matching performance among these virtual user sets is not significant. The clustering of these ROC curves seems to support the independence assumption between the face and fingerprint modalities, thereby validating the use of virtual subjects. Garcia-Salicetti et al., 2005 also report similar results for experiments on a subset of the BIOMET multimodal database (Garcia-Salicetti et al., 2003). However, experiments by Poh and Bengio, 2005c seem to indicate that the recognition performance of a multimodal biometric system evaluated on a virtual multimodal database is significantly different from the results obtained on a true multimodal database. Hence, the issue of using virtual versus true multimodal databases to evaluate the performance of a multibiometric system needs further investigation.

Figure A.1. ROC curves of the multimodal (face and fingerprint) biometric system for the 1,000 virtual user sets randomly created by Indovina et al., 2003. The variation in matching performance among these virtual user sets is not significant which seems to validate the use of virtual users.

Another issue unique to multibiometric system evaluation is the testing of a cascaded multibiometric system, where multiple sources of biometric information are processed in a sequential order (see Chapter 2 for more details). The cascading scheme can improve user convenience as well as allow fast and efficient searches in large scale identification tasks. Further, a hierarchical
processing architecture (mixture of cascade and parallel processing sequences) is also possible in a multibiometric system. Evaluation of cascaded or hierarchical multibiometric systems is more complex because of the trade-off between user convenience and security offered by such systems. Standard protocols are not available to evaluate cascaded or hierarchical multibiometric systems.

A.3 Multimodal biometric databases

A good multimodal biometric database must be representative of the population and each biometric trait must preferably exhibit realistic intra-class variations (achieved by collecting data over multiple sessions spread over a period of time and in different environmental conditions). One must also carefully decide which biometric traits and sensors to use and how many samples per user per trait needs to be collected. Further, due to the involvement of human subjects, legal and privacy issues must also be considered and approval of organizations like the Institutional Review Board (IRB) is mandatory in many countries (Penslar, 1993). This makes the collection of a true multimodal biometric database a time consuming and complicated process. In this section, we introduce some of the multimodal biometric databases that are available in the public domain. The following eight databases are true multimodal databases collected at various universities and research laboratories around the world.

1 BT-DAVID (British Telecom Laboratories - Digital Audio-Visual Integrated Database):
   BT-DAVID (Mason et al., 1996) is a bimodal audio-visual database, which contains synchronized video and audio data obtained from more than 100 subjects. Of these 100 subjects, data from 30 subjects was recorded on five sessions spaced over several months. The video recordings include frontal and profile views of the subject's face with different illumination conditions and background scenes. The audio samples correspond to different utterances, including the English digit set, English alphabet E-set and vowel-consonant-vowel phrases. Portions of this database also include lip highlighting. Apart from its use in the development of biometric (audio-visual speaker recognition) algorithms, the BT-DAVID database can also be used to study a variety of research themes such as facial image segmentation in video, audio-visual speech recognition, speech-assisted video coding and synthesis of talking heads.

2 M2VTS (Multi Modal Verification for Teleservices and Security applications) database:
   The M2VTS database (Pigeon and Vandendrope, 1996) is another bimodal audio-visual database consisting of synchronized video and audio data of 37 subjects. This database contains five shots for each subject recorded at one week intervals in ideal conditions (good picture quality, indoor environment, nearly uniform illumination and uniform background). During each shot, the subject utters the digits '0' to '9' in his/her native language (mostly French) and rotates the head by 90 degrees towards the left and the right.

3 XM2VTS (Extended Multi Modal Verification for Teleservices and Security applications) database: The XM2VTS database (Messer et al., 1999) is a bimodal biometric database with face and voice modalities. It consists of synchronized video and audio data as well as image sequences corresponding to multiple views of the subject's face. This database has video and speech recordings of 296 subjects collected over a period of four months. The recordings were carried out in four sessions at one month intervals with two recordings of the subject in each session. Uniform illumination and a plain blue background were used during the recording. The subject was asked to read three sentences (two digit sequences along with a phonetically balanced sentence) and a video of the frontal face was recorded as the subject reads the sentences. Subsequently, the subject was asked to rotate his/her head from the center to the left, right, up and down before finally returning to the center. Based
on the XM2VTS database, Poh and Bengio, 2005a have developed a benchmark database of match scores that can be used to compare different score level fusion techniques. Eight baseline biometric matchers (five for face and three for voice) were used to generate the match scores in the benchmark database.

4 **BANCA database:** The BANCA database (Bailly-Bailliere et al., 2003) is a challenging bimodal audio-visual database recorded in three different scenarios, namely, controlled, degraded and adverse. Audio and video data from 208 subjects was obtained over a period of three months. For each of the four different native languages (English, French, Italian and Spanish), video and speech data were collected from 52 subjects over 12 sessions. In the first four sessions, the video was recorded in controlled conditions using a high quality digital camera with uniform illumination and plain background. The next four sessions correspond to the degraded scenario where the video was recorded using an analog web camera. The final four sessions were recorded in adverse conditions using the high quality digital camera with changes in illumination and complex background scenes. In each of the 12 sessions, the subject was prompted to say a random 12 digit number, his/her name, address and date of birth. The audio data was recorded using both a low quality and a high quality microphone.

5 **BIOMET multimodal database:** The BIOMET multimodal database has five biometric modalities, namely, face, voice, fingerprint, hand image and online-signature (Garcia-Salicetti et al., 2003). This database was collected in three different sessions with three and five months spacing between them. The number of subjects in the three sessions was 130, 106 and 91. The face database includes video recordings of the frontal and profile views of the face, the frontal face images of the subject captured using an active differential imaging device (referred to as “Infrared Camera device” in Garcia-Salicetti et al., 2003) and facial surface data captured using a 3D acquisition system. The video recordings also have synchronized audio recordings of the subject pronouncing his/her identification number, digits 0 to 9, “oui”, “non”, and 12 phonetically balanced sentences in French. Two-dimensional images of the subject’s left hand were captured using a scanner. The x and y coordinates (over time) of the subject’s signature were recorded at a rate of 200 Hz using a digitizing tablet. Along with the x and y coordinates, the pressure applied on the writing device, the azimuth and the altitude of the pen were also recorded. Optical and capacitive fingerprint sensors were used to capture images of the index and middle fingers of the subject’s right hand.

6 **MCYT (Ministerio de Ciencia y Tecnologia, Spanish Ministry of Science and Technology) baseline corpus:** The MCYT bimodal database (Ortega-Garcia et al., 2003) has face and signature biometric modalities collected from 330 subjects. Fingerprint images of all 10 fingers were collected using both optical and capacitive sensors. Twelve impressions were collected for each finger on both the sensors. In the case of signature modality, 25 samples were collected for each subject. Further, for each subject 25 highly-skilled forgeries were obtained. Both online signature information such as the trajectory (x and y coordinates) of the pen, pen pressure and pen azimuth/altitude and offline information (image of the signature) are stored in the database.

7 **UND (University of Notre Dame) biometric database:** The UND biometric database (Flynn et al., 2005) is a collection of several small multimodal databases with face and ear modalities. Since the images in this database were captured using cameras operating in the visible and infra-red spectral regions and a 3D range scanner, this database can also be used for the design and evaluation of multi-sensor biometric systems. The number of subjects in this database varies from 80 to 350. A subset of the UND biometric database has been used in the Face Recognition Grand Challenge (FRGC) experiments (Phillips et al., 2005). The FRGC database includes high resolution 2D still face images obtained in controlled (studio
setting) and uncontrolled (e.g., hallways and outdoors) illumination conditions as well as 3D face images obtained using a range scanner.

8 **NIST BSSR1 (Biometric Scores Set - Release 1):** The NIST BSSR1 (National Institute of Standards and Technology, 2004) is a multimodal biometric match score database. The NIST BSSR1 consists of fingerprint and face match scores of 517 subjects. Note that face and fingerprint images of the subject are not available. One fingerprint score was obtained by comparing a pair of impressions of the left index finger and another score was obtained by comparing impressions of the right index finger. Two different face matchers (referred to as ‘C’ and ‘G’) were applied to compute the similarity between two frontal face images. So, there are four match scores for each subject (one for each modality). Although the number of subjects in the NIST BSSR1 is the largest among all the public-domain true multimodal biometric databases, there are only two samples per subject. Thus, only a single genuine match score is available for a subject in each modality.

Apart from the eight multimodal biometric databases described above, several unimodal biometric databases are also available in the public domain. Some of the commonly used unimodal biometric databases are the Fingerprint Verification Competition (FVC) databases (Maio et al., 2002; Maio et al., 2004), the Carnegie Mellon University Pose, Illumination, and Expression (CMU-PIE) face database (Sim et al., 2003), the FERET face database (Phillips et al., 2000b) and the Chinese Academy of Sciences - Institute of Automation (CASIA) iris image database (Ma et al., 2003). These unimodal biometric databases can be used for evaluating multi-sensor, multi-instance, multi-sample and multi-algorithm biometric systems.
References


REFERENCES


REFERENCES


REFERENCES


1046, Rhodes.


Fancourt, C. L., Bogoni, L., Hanna, K. J., Guo, Y., Wildes, R. P., Takahashi, N., and Jain,
U. (2005). Iris Recognition at a Distance. In *Fifth International Conference on Audio- and
Video-based Biometric Person Authentication (AVBPA)*, pages 1–13, Rye Brook, USA.

In *Sixteenth International Conference on Pattern Recognition (ICPR)*, volume 2, pages 382–
385, Quebec City, Canada.


Feng, G., Dong, K., Hu, D., and Zhang, D. (2004). When Faces are Combined with Palmprints:
A Novel Biometric Fusion Strategy. In *First International Conference on Biometric Authen-
tication (ICBA)*, pages 701–707, Hong Kong, China.

Quality in Multi-algorithm Fingerprint Verification. In *IAPR International Conference on
Biometrics (ICB)*, pages 213–220, Hong Kong, China.

Bayesian Adaptation for User-Dependent Multimodal Biometric Authentication. *Pattern

On-line Signature Verification System based on Fusion of Local and Global Information. In *Fifth International Conference on Audio- and Video-based Biometric Person Authentication
(AVBPA)*, pages 523–532, Rye Brook, USA.


Database. Available at http://www.nd.edu/~cvrl/UNDBiometricsDatabase.html.


Fuentes, M., Garcia-Salicetti, S., and Dorizzi, B. (2002). On-line Signature Verification: Fusion
of a Hidden Markov Model and a Neural Network via a Support Vector Machine. In *Eighth
International Workshop on Frontiers in Handwriting Recognition*, pages 253–258, Ontario,
Canada.


Garcia-Salicetti, S., Beumier, C., Chollet, G., Dorizzi, B., Jardins, J. L. L., Lunter, J., Ni, Y., and
Including Face, Voice, Fingerprint, Hand and Signature Modalities. In *Fourth International
Conference on Audio- and Video-based Biometric Person Authentication (AVBPA)*, pages
845–853, Guildford, UK.

for Multibiometric Systems Evaluation on Virtual and Real Subjects. In *Fifth International
REFERENCES

Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), pages 494–502, Rye Brook, USA.


Han, J. and Bhanu, B. (2005). Gait Recognition by Combining Classifiers Based on Environmental Contexts. In Proceedings of Fifth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), pages 416–425, Rye Brook, USA.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Index

Abstract level fusion, see Decision level fusion
Acceptability, 19
Acquisition sequence, 42, 51
Ancillary information, 143
AND rule, 50, 74
ANSI X9.84, 31
Authentic score, see Genuine score
Authentication, 8

BANCA multimodal database, 177
Bayes rule, 76, 93, 103, 166
Bayesian decision fusion, 75
Bayesian decision theory, 93, 98, 167
Behavior Knowledge Space, 81
Behavioral characteristics, 1
Belief function, 79
Bertillonage system, 3, 162
Best practices, 174
BioAPI, 31
BIOMET multimodal database, 175, 177
Biometric applications, 17
commercial, 17
forensic, 17
government, 17
Biometric authentication, see Biometrics
Biometric characteristics, see Biometric traits
Biometric standards, 29
Biometric traits, 3, 19
Biometrics, 1
Biweight estimators, 118
Borda count method, 57, 72
Branch-and-bound search, 68
BT-DAVID, 176

Canny edge detector, 151
CBEFF, 30
Challenge-response mechanism, 29, 41
Circumvention, 19
Class conditional density, 100
Classifier
balanced, 137
imbalanced, 137
Classifier combination rules, 93–97
Classifier ensembles, 37
Classifier-based score fusion, 99, 124
Coherence, 150
Conditional independence, 77
Confidence level fusion, see Score level fusion
Confusion matrix, 76
Consensus aggregation, 37
Continuous monitoring, 41
Cooperative agents, 37
Copula models, 108
multivariate Gaussian, 108
Correlation, 83, 108, 109
matrix, 108
Covariance matrix, 109, 150
Cumulative Match Characteristic curve, 16
Curse of dimensionality, 49, 66
d-prime value, 15
Decimal scaling, 115
Decision boundary, 124
Decision level fusion, 57, 73
Decision profile, 79
Decision template, 79
Decision-making, 7
Degree of belief, 78
Dempster-Shafer theory of evidence, 78
Density estimation
Gaussian kernel, 106
non-parametric, 100, 102, 103, 105
parametric, 100
Density-based score fusion, 98, 99
Detection Error Tradeoff curve, 12
Dimensionality reduction, 66, 68
Directional histogram, 149
Discriminant function, 75, 77, 90, 167
Dissimilarity measure, see Distance score
Distance score, 10, 91
INDEX

Distance-to-similarity transformation, 119
Distribution function, 99, 105
Diversity measures, 83
Divide-and-conquer classifiers, 37
Doddington’s zoo, 13
Double sigmoid normalization, 116
Dual-factor authentication, 1, 49
Durbin test, 15
Dynamic classifier selection, 37, 56

Efficiency, 114
Enhancement, 59
Enrollment, 7
Equal Error Rate, 15
Ethnicity, 143
classifier, 164, 170

F-test, 15
Face, 21
Face modeling, 63
Failure to Acquire Rate, 15
Failure to Capture Rate, see Failure to Acquire Rate
Failure to Enroll Rate, 15
Fake biometric trait, 29
False Accept Rate, 10
False Match Rate, see False Accept Rate
False Non-Match Rate, see False Reject Rate
False Reject Rate, 12
Fault tolerance, 42
Feature dimensionality, 31
Feature extraction, 6
Feature level fusion, 55, 64
Feature normalization, 67
Feature selection, 68
Feature transformation, 68
Filtering, 162
Fingerprint, 21
image quality, 148
Functionality creep, 33
Fusion, see Information Fusion

Gait, 24
Gallery images, 7
Gender, 143
classifier, 164, 170
Generalized densities, 105
Genuine Accept Rate, 12
Genuine score, 10
Genuine user, 8
Goats, 13

Hampel influence function, 118
Hand geometry, 22
Height, 143
Highest rank method, 57, 71
Hough transform, 151
Human computer interface, 42

Hybrid methods, 37
Hybrid systems, 49

IAFIS, 19
Identical twins, 21
Identification, 8
Identification rate, 16
rank-k, 16
Identifiers, see Biometric traits
Identity, 1, 35
management, 1
Impostor, 8
Impostor score, 10
INCITS M1, 30
Independence, 93, 94, 103
Independent Component Analysis, 68
Indexing, 3
Indicators, see Biometric traits
Information fusion, 32, 38
after matching, 55
prior to matching, 55
Information limitation, 33
Input images, see Probe images
Integration of evidence, see Information fusion
Inter-class similarities, 25
Inter-class variations, 10
Interoperability, 26
Intra-class variations, 10, 25
Invariant representation, 59
Iris, 23
image quality, 151
ISO/IEC JTC1 SC37, 30
Iterative Closest Point algorithm, 61

Joint probability density, 93, 103
Keystroke dynamics, 23
Knowledge-based mechanisms, 1
Kruskal Wallis test, 15

Lambs, 13
Layered biometrics, 32
Levels of fusion, 55
Likelihood ratio, 104
Likelihood ratio test, 104
Linear Discriminant Analysis, 68, 165
Liveness detection, 28
Logistic function, 116
Logistic regression, 57, 72

M2VTS multimodal database, 125, 176
MAD, see Median absolute deviation
Majority voting, 74
Marginal-derived quality, 156
Marginal density, 93, 103
Match score, 8, 91
Matcher, 7
Matcher limitation, 34
Max rule, 96
Max score fusion, 113
Maximum likelihood estimation, 101
MCYT bimodal database, 158, 177
Mean rule, 95
Measurability, 19
Measurement level fusion, see Score level fusion
Median absolute deviation, 67, 116
Median normalization, 67, 116
Median rule, 97
Min rule, 96
Min score fusion, 113
Min-max normalization, 67, 114
Minimum error-rate classification rule, 93
Minutia points, 65
Mixture of experts, 37
Modalities, see Biometric traits
Mosaicing, 7, 60
  face, 61
  fingerprint, 60
Multi-algorithm systems, 46
Multi-instance systems, 47
Multi-sample systems, 48
Multi-sensor systems, 44
Multi-unit systems, see Multi-instance systems
Multibiometric systems, 32, 40
Multidimensional scaling, 68
Multimodal biometric database, 176
Multimodal biometric systems, 49
Multiple classifier systems, 37, 58

Naïve Bayes rule, 77
Negative recognition, 2
Neyman-Pearson theorem, 104
NIST BSSR1 database, 12, 111, 128, 178
Noise, 25, 41, 143
Non-homogeneity, 91, 114
Non-repudiation, 3
Non-universality, 25, 41

One-to-many comparison, 8
One-to-one comparison, 8
Operational evaluation, 174
Opinion pool, 37
OR rule, 74
Order statistics, 113, 137

Palmprint, 22
Particle swarm optimization, 78
Parzen window, 102
Passwords, 2
Pattern recognition system, 5
Performance, 19, 173
Performance disparity, 83
Permanence, 19
Physical characteristics, 1

Positive recognition, 8
Power spectrum, 151
Principal Component Analysis, 68
Privacy, 33
Privacy-Enhancing Technologies, 33
Probe images, 7
Processing sequence, 42, 52
  cascade, see serial
  hierarchical, 53
  parallel, 52
  serial, 52
Product rule, 94

Quality assessment, 6, 148
Quality-based fusion, 143, 156
Query images, see Probe images

Rank level fusion, 57, 70
Receiver Operating Characteristic curve, 12
Recognizability, 13
Registration, 46
Rejection, 9
Representation limitation, 34
Return on investment, 173
Robustness, 114

Scenario evaluation, 174
Score level fusion, 57, 91
Score normalization, 99, 113, 114
  user-specific, 134
Segmentation, 46
Sensor, 5
Sensor fusion, 37
Sensor level fusion, 55, 60
Sequential backward floating search, 68
Sequential backward selection, 68
Sequential forward floating search, 68
Sequential forward selection, 68
Sheep, 13
Signature, 23
Similarity score, see Match score
Sklar’s theorem, 108
Smart cards, 33
Social choice functions, 37
Soft biometric likelihoods, 168
Soft biometrics, 143, 162
Sources of biometric information, 42, 44
Spoof attacks, 28, 41
Stacked generalizations, 37
Standards, see Biometric standards
Stored images, see Gallery images
Strong biometric, 83
Sum of scores fusion, 113
Sum rule, 94
Support vector machine, 157
System database, 7
System evaluation, 173
Tanh normalization, 117
Technology evaluation, 173
Template, 7
Template improvement, 65
Template update, 65
Threshold, 8, 10, 131
user-specific, 133
Throughput rate, 16
Token-based mechanisms, 1
Tokens, 2
Transformation-based score fusion, 99, 113
Trojan horse program, 29
True multimodal database, 174
Two-quadrics, 116

UND biometric database, 177
Unibiometric systems, 34
Uniqueness, 19
Universality, 19
US-VISIT program, 18
User acceptability, 173

User acceptance, see Acceptability
User-specific score fusion, 131
User-specific weights, 134

Verification, 8
Virtual multimodal database, 174
Voice, 24
Vulnerability, 29, 173

Watchlist, 17
Wavelet, 153
Weak biometric, 83
Weight, 143
Weighted majority voting, 75
Weighted sum rule, 113, 158
Wolves, 15

XM2VTS multimodal database, 127, 128, 176

Z-score normalization, 115
Zero-one loss function, 93