Fingerprint and Face Identification for Large User Population

Teddy Ko and Rama Krishnan

Lockheed Martin
1120 Vermont Avenue, NW – 5th Floor
Washington DC 20005
teddy.ko@lmco.com & rama.krishnan@lmco.com

Abstract

The main objective of this paper is to present the state-of-the-art of the current biometric (fingerprint and face) technology, lessons learned during the investigative analysis performed to ascertain the benefits of using combined fingerprint and facial technologies, and recommendations for the use of current available fingerprint and face identification technologies for optimum identification performance for applications using large user population. Prior fingerprint and face identification test study results have shown that their identification accuracies are strongly dependent on the image quality of the biometric inputs. Recommended methodologies for ensuring the capture of acceptable quality fingerprint and facial images of subjects are also presented in this paper.

Keywords: Fingerprint Identification, Face Identification, Biometrics Systems, Statistical Pattern Recognition, and Machine Intelligence.

1. Introduction

Biometrics, which is the biological measurement of any human physiological or behavioral characteristics, can be used to make personal identification provided it has the following desirable properties [1][9]:

1. **Universality**, which means that every person should have the characteristics.
2. **Uniqueness**, which indicates that no two persons should have the same physical characteristics.
3. **Permanence**, which means that the characteristics should be invariant with time.
4. **Collectability**, which means that the characteristics can be measured quantitatively.

In practice, there are some other important requirements [2][9]:

1. **Performance**, which refers to the achievable identification accuracy, the resource requirements to achieve acceptable identification accuracy, and the operational or environmental factors that affect the identification accuracy.
2. **Acceptability**, which indicates to what extent people are willing to accept the biometric system.
3. **Circumvention**, which refers to how easy it is to fool the system by fraudulent techniques.

Biometric identification systems, which use physical characteristics to check a person's identity, ensure much greater security than password and number systems. Examples of biometrics [2] include face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice, ear, facial thermograms, odor, gait, and DNA. There are two important utilization of biometric systems: (1) Authentication or verification of a person's identity, i.e., a person proves that he/she is the person who he/she claims to be and (2) identification in which a person's identity is sought using the existing enrolled biometrics database.

However, each biometric technology has its strengths and limitations, and no single biometrics is expected to effectively satisfy the requirements of all identification or authentication applications. A brief comparison of major biometric techniques that are widely used or under investigation can be found in [2]. A single biometric sometimes fails to be accurate enough for the identification of an entire population. Another disadvantage of using only one biometrics is that the physical characteristics of a person for the selected biometric might not be always available or readable.

1.1 Multi-Modal Biometrics

Multi-modal biometrics refers to the use of a combination of two or more biometric modalities in a single identification system. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. One is that different biometric modalities might be more appropriate for the different identification applications. For example in a home banking application, a customer might enroll both fingerprint and voice. Then, the fingerprint can be used from a home or laptop sensor; while voice and a personal identification number (PIN) can be used over the phone. Another reason is simply customer preference. For instance, an automatic teller machine could offer fingerprint, face, and eye biometrics, or a combination of two of these for customer to choose.

Although fingerprints can be combined with other modalities, there are reasons to suggest that this would not be the first biometric to require complementing. One reason is that, along with other biometric systems, fingerprint systems already have very high recognition rates. This contrasts with less reliable modalities, where combining one with another biometric modality or with a PIN is more advantageous. Another reason is that a single person has up to ten statistically independent samples in ten fingers, compared to two for eye and hand, and one for face, voice, and signature.

Recognition rate will be a deciding factor in acceptance for demanding applications such as automatic teller machines (requiring a very low rate of false rejections), and department of defense (DOD) applications (requiring a very low rate of false acceptances). For especially demanding applications, multi-modal systems combining biometrics will provide an optimum level of security and convenience to users. Alternatively, multiple verifications, such as by using multiple fingers of a subject, can be used to enhance recognition reliability.

Recent test results of biometric accuracy determination using large-scale databases performed by U.S. Government and its contractors have shown that fingerprints provide a higher accuracy rate than face images in both verification and identification [3]. Using realistic INS data, one index flat-fingerprint can provide a 95% probability of verification with 1% of false acceptance for verification using statistical samples of 3000 fingerprints. Using realistic face data, tests show that the best commercial facial recognition systems available can attain a 90% probability of verification with 1% probability of false acceptance for verification using statistical samples of 3000 faces. Both these results are strongly affected by the image quality of the biometric.

It has also been established in [3] that all subjects can not be successfully identified using single fingerprint biometric with existing fingerprint technology for the wide range of conditions expected in real life applications. Tests by NIST using INS data show that for approximately 2% of the fingerprints in the INS database the friction ridges are too damaged to be matched with existing technology. In addition, within the intelligence community, facial data is often the only biometric data that has been and is currently being captured. Face data is one key source for “watch lists.” Fingerprint data cannot be captured in many situations used to construct “watch lists.” The recent NIST biometric study [3] concluded that a dual biometric system using one or more fingerprint images and a face image is needed to meet projected future identification requirements.

The biometric test studies have shown that use of multiple biometrics will be required for achieving acceptable identification accuracy for large user population identification applications. This paper presents the recommended methodologies for using a combined fingerprint and facial biometric identification technologies to achieving optimum identification performance for a large user population identification application.

1.2 IDENT and IAFIS

IDENT is the abbreviation of the United States Immigration and Naturalization Service (INS) Automated Biometric Identification System. IDENT is world’s largest media (rolled, flat fingerprints, and facial images) biometric database. The system has approximately 1,800 terminals at around 600 unique locations. It has over 20,000 peak load daily transaction, and access to 16 million continuously growing records. IDENT provides a cost-effective means of rapid identification based on the use of biometric data. The key objective of IDENT is to rapidly establish the identity of an individual encountered by the INS during enforcement processing or benefit servicing processes. The Federal Bureau of Investigation's (FBI's) Integrated Automated Fingerprint Identification System (IAFIS) provides identification services to the nation's law enforcement community and to organizations where criminal background histories are a critical factor in consideration for employment. The IAFIS provide services, such as, ten-print, latent print, and subject search, to FBI Service Providers, and federal, state, and local law enforcement users.

1.3 Objective

The main challenge in a biometric system is how to reduce the error rates to as low as possible, how to make it operate successfully for the entire user population for the given application, and how to ensure that it will not be compromised. The main objective of this paper is to present the state-of-the-art of the current biometric (fingerprint and face) technology, lessons learned during the investigative analysis performed to ascertain the benefits of using combined fingerprint and facial technologies and recommendations for the use of current available fingerprint and face identification technologies for optimum identification performance for applications using large user population.

The recommended approaches for using the currently available fingerprint and face identification technology for achieving optimum identification performance characteristics for large user population applications are presented in this paper. This will include recommended methodologies for using the combined fingerprint and facial biometric technologies (operating in series or in parallel modes) for the user identification process. Prior fingerprint and face identification test study results have shown that their identification accuracies are strongly dependent on the image quality of the biometric inputs. Recommended methodologies for ensuring the capture of acceptable quality fingerprint and facial images of subjects are also presented in this paper.

2. Fingerprint Identification

Fingerprints, which have been used for about 100 years, are the oldest biometrics of identity. The foundations of modern fingerprint identification were established by the studies of Sir F. Galton and E. Henry at the end of nineteenth century. A fingerprint is formed of composite curve segments. The light areas of the fingerprints are called ridges while the dark areas are called valleys. Galton’s study introduced the minutiae, which are the local discontinuities in the ridge flow pattern, as discriminating features and show the uniqueness and permanency of minutiae. Henry’s study examined the global structure of fingerprints and established the famous “Henry System” of fingerprint classification, which is an effective method of indexing fingerprints, and is still in use in most identification systems.

By using the ideas presented above, fingerprints are partitioned by the Henry Classification and fingerprint matching is carried out by comparing Galton Features. After Henry and Galton, work on fingerprint identification and its specification was extended and refined. But most of extended features are not used in the current automated fingerprint identification systems (AFIS). Instead, in accordance with the FBI representation of fingerprints [5], ridge endings and bifurcations are taken as the distinctive features of fingerprints. In this method, the location and angle of the feature are taken to represent the fingerprint and used in the matching process. Together with these, fingerprints contain two special types of features called core and delta points. These points are often referred to as singularity points of a fingerprint. The core point is generally used as a reference point for coding minutiae and defined as the topmost point on the innermost recurving ridge.

In an AFIS, the input is just a fingerprint or up to ten fingerprints and the output is a list of potential match candidate subjects, whose fingerprints were found to be similar to the searched fingerprint inputs based on the fingerprint match scores.

2.1 Fingerprint Image Acquisition

The oldest and most common method of capturing a fingerprint image is to obtain an impression by rolling an inked finger on paper and then scanning it using a flatbed scanner. This method may result in highly distorted fingerprint images and thus it should be carried out by a trained professional. Another common method of obtaining fingerprint images is to scan the image directly using a CCD camera. The live scan method provides better images and does not need expertise, but highly distorted images are still possible because of dryness of skin, skin disease, sweat, finger pressure, dirt or humidity. In both of these methods, the image acquired is a high-resolution 500 dpi grayscale image of the fingerprint. In all of the available methods, the following variations are possible between two different acquisitions of the same fingerprint [7]:

- Translation because of different positioning of the fingerprint on the input device.
- Rotation due to different positioning of the fingerprint on the input device.
- Spatial scaling because of different downward pressure on the surface.
- Contrast difference because of different downward pressure and ink density in ink-based methods.
- Different regions of the same fingerprint are captured in different acquisitions. Impressions are usually only a partial description of the whole fingerprint.
- Shear transformation as the finger may exert a different shear force on the surface.
- Local perturbation, i.e., local translation, rotation or scaling because of non-uniform pressure and shear force.
- Breaks or smudges caused by non-uniform contact and non-uniform ink density in ink based methods.
- Nonpermanent or semi-permanent distortions like skin disease, scars, sweat, etc.

2.2 Fingerprint Matching

Matching is the process of measuring the similarity between two fingerprint images. The most commonly used matching method is minutiae based matching. But there are also other approaches. There are two approaches in minutiae based matching: point matching and structural matching. In point matching, two sets of minutiae code using their locations are aligned and the sum of similarity between the overlapping minutiae is calculated. The similarity between two minutiae is measured using the attributes of the minutiae. Alignment is an important problem in point matching and this is affected by the registration process in most of the systems. In structural matching, the locations are mostly discarded and a graph, which codes the relative locations of minutiae, is constructed. The subgraphs around each minutia are used to build feature vectors. As the locations are discarded, alignment is not needed.

2.3 Performance Criteria

In biometric matching studies, the performance of the system is given by the accuracy of the system. In a biometric decision, a type of Yes/No pattern recognition decisions, there are four possible outcomes: True Accept (TA) or called correct accept, False Accept (FA), False Reject (FR), and True Reject (TR) or called correct reject. FA and FR are errors, while TA and TR are correct outcomes sought in a biometric system. False Accept Rate (FAR) and False Reject Rate (FRR) are widely used standard metrics of the verification accuracy of biometric systems. The performance of a biometric system are usually shown as a Receiver Operating Characteristic (ROC) curve that plots the true accept rate vs. false accept rate at different match score thresholds. By manipulating the decision criteria, the relative probabilities of these four outcomes can be adjusted in a way that reflects their associated costs and benefits [8]. These may be very different for different applications. For example, in a customer context, the cost of FR error may exceed the cost of FA error, whereas just the opposite may be true in a more secure DOD application.

Reliability and uniqueness of features are two dominant parameters, which contribute to FARs and FRRs in automated fingerprint identification/authentication. While most methods for testing fingerprint identification systems revolve around determining the FRR and FAR, these error rates can be misleading. In addition to factors such as software algorithm performance and scanner characteristics, fingerprint quality of individuals and of database population, as well as conditions inherent in certain applications (e.g., environment, posture, frequency of use, etc.) determine the performance of fingerprint identification.

There is a common and intuitive assumption that the use of multiple fingerprints or multiple biometrics must improve performance, because surely more information is better than less information. On the other hand, a different intuition suggests that if a strong biometric modality is combined with a weaker one, the resulting decision is in a sense averaged (and hence will be degraded from the performance that would be obtained by relying solely on the stronger biometric modality). There is truth in both intuitions. There are two possible ways to combine the outcomes of multiple biometric tests by forming conjunctive or disjunctive decisions [8]. In conjunctive rule, the subject is required to pass all of the biometric tests. In disjunctive rule, the subject will be accepted if passing at least one of the biometric tests. The key to resolving the paradox is that when two biometric tests are combined, one of the resulting error rates (FAR or FRR) becomes better than the stronger of the two tests, while the other error rate becomes worse than that of the weaker of the tests. This is also true for accurate rates of TAR and TRR. The above statement can be easy understood using statistical concept [4].

2.4 Asymmetric Matching

The IDENT system searches files of Lookout, Apprehension, Border Crossing Card and Asylum subject fingerprints. Each IDENT search uses the two index flat fingers, while IAFIS searches use the ten rolled fingerprints. Recent biometric studies have also shown that asymmetric matching (matching of mixed impression type fingerprints – flat print to rolled print and vice versa) results in degraded accuracy compared to matching of same impression type (flat print to flat print or rolled print to rolled print) prints. Therefore the way fingerprints are captured becomes critical when integrating multiple fingerprint identification systems. Asymmetric matching causes more false positives, which waste time to examine, and more false negatives, which result in missed identification of true mates. The recommended solution is to use the same rolled finger impressions for all integrated systems.

3. Face Identification

Face recognition is the identification of subjects by the unique characteristics of their faces. In general, face recognition is a three-step procedure [7]. It starts with a picture of the subject, attempting to find a person in the image. The face recognition system locates the head and then the eyes of the individual. A matrix (or called face signature) is then developed based on the characteristics of the individual's face. The method of defining the matrix varies according to the different algorithm. The matrix is then compared to matrices that are in the database and a similar score is generated for each comparison.

For face recognition, as well as other biometric systems, there are two types of comparisons. The first is verification, where the biometric system compares the given individual with who that individual says they are and gives a yes/no decision. The second is the identification, where the biometric system compares the given individual to all individuals in the database and gives a ranked list of matches.

3.1 Face Match Evaluation Study

In order to find out the feasibility of facial recognition technology for use in the IDENT system, the INS sponsored an evaluation of leading commercially available facial recognition technologies in the industry. The facial recognition products from three leading vendors, and each representing one of three major recognition technologies – Vendor1 based on local feature analysis, Vendor2 based on neural network technology, Vendor3 derived from the eigen face technology – were used for this evaluation test.

The intent of the evaluation test was to determine the accuracy performance of the face matching algorithms using the actual photo images stored in the production IDENT system. The match results of the evaluation test were then analyzed to determine the feasibility of using facial recognition technology as the secondary match process for the IDENT system.

In order to evaluate the different face recognition technologies, photo images from the actual operational IDENT system were used for the test. A representative test sample of approximately one hundred photo image pairs, containing photo images of the same subject taken a different times, were used for the test. These were derived from the Recidivist hits across the US border. The photo image pairs where manually verified to ensure that they were from the same subjects, providing ground truth data for the test. One set of the photo image pairs was used as the "Search" set and the other set as the "File" set.

The photo images were of mixed quality and include frontal and non-frontal images. There are changes in photo images from variations in pose, lighting conditions, and background complexity. This variation resulted from the disparate photo image capture environments present at different INS capture sites. In order to make an accurate and valid assessment of the performance of the face recognition technologies, the photo images were categorized as "good" and "poor" photo images by visual examination. A breakdown of the search set used for the evaluation test is given in Table 1.

Category	Sub-total	Comments
Good quality	58	Full frontal views with good positioning of the head within the captured photo image
Pose variation	39	Images with variation in pose
Light problem	3	Images were either too dark or had reflections on the faces
Multi faces	3	Presence of multiple subjects in the photos
Capture problem	3	Blurry images and images with partial head capture
Total	106	

Table 1: Composition of facial image search sample used for test.

There were 91 males and 15 females in the search test. The 106 search images came from 100 unique individuals and included duplicate images of some of the individuals captured at different times). There where 100 facial images in the file set corresponding to the unique individuals in the search set. Every search set image had a corresponding unique mate in the file. The match performance accuracy was calculated separately for both the complete photo set and the good quality photo set for accurate assessment of the face recognition technology. This was done in recognition of the fact that the IDENT photo images had typically been acquired from uncontrolled operational environments. Some of the sites did not have the proper lighting and background environments for the capture of acceptable quality facial images.

Each photo images in the search set was then matched against the complete file database and the match score for the top candidates were saved for subsequent identification match analysis. This was repeated for each vendor, using their feature extraction and matching software. The results of the evaluation test for the three selected vendors are shown in Table 2. The results show that among the vendors, Vendor1 had the best performance in the test, and had correct identification of 80.2% for the complete database and 93% for the good quality database. The match accuracy rates were calculated for: (1) Top rank match (where the correct subject was in the top rank position with the match score above the match threshold); (2) Top candidate list match, where the correct subject was in the top candidate list with the match score above the threshold, but not in the top rank position.

	Vendor1	Vendor2	Vendor3
Complete photo image set			
Correct matches			
Correct subject in the top rank position	41.5%	5.7%	19.8%
Correct subject in the top candidate list 2-5	38.7%	7.5%	20.8%
Correct match sub-total	80.2%	13.2%	40.6%
Missed matches			
Missed matches with wrong subjects in the candidate list and right subject not in candidate list.	14.1%	30.2%	59.4%
Missed matches with no candidate list.	5.7%	56.6%	0%
Total	100%	100%	100%
Good quality photo image set			
Correct matches			
Correct subject in the top rank position	63.8%	8.6%	22.4%
Correct subject in the top candidate list 2-5	29.3%	12.1%	27.6%
Correct match sub-total	93.1%	20.7%	50%
Missed matches			
Missed matches with wrong subjects in the candidate list and right subject not in candidate list	5.2%	32.7%	50%
Missed matches with no candidate list	1.7%	46.6%	0%
Total	100%	100%	100%

Table 2: Facial match test results.

A visual analysis of the photo image pairs, which were not positively identified by the Vendor1's system, showed that most of these images had significant variation in the presentation of the face in size and tilt. It was recognized that institution of quality control procedures in the photo capture process would enable the capture of acceptance quality photo images for positive facial identification.

3.2 Face Match Feasibility Study

An expanded facial match test was performed for the facial recognition feasibility study using the product of the leading facial recognition technology in the initial evaluation study. A secondary facial match was performed for all the search/file candidates that were found to be positive matched by the primary fingerprint matcher system in the operational IDENT system. The facial match was performed for: (1) Recidivist and Lookout match candidates resulting from searches initiated from the field sites; (2) Lookout match candidates resulting from the lookout load search initiated from the INS Biometric Center. The facial match test was conducted over a two-month period, from December 1998 to January 1999. The composition of the match test performed for the expanded facial match test is given in Table 3.

Search type	Search facial image source	File facial image source	Total matches performed in the test
Field search on RC database	Live image from IDENT client	Live image from IDENT client	45,477
Field search on LO database	Live image from IDENT client	Photo from FD 249 card	2,715
Lookout Load search on LO database	Photo from FD 249 fingerprint card	Photo from FD 249 card	482

Table 3: Facial matches performed for the expanded match test.

The facial match test results were analyzed independently for the true positive fingerprint match pair (fingerprint matches which were confirmed as true matches by the INS agents) and false fingerprint matches (fingerprint matches which were confirmed as false match by the INS agents) to assess the effectiveness of the secondary facial match process.

The results of the secondary facial match observed for expanded feasibility study are provided in Table 4. The test results shown included only the results associated with Recidivist match candidate pairs. The Lookout matches did not provide a valid test sample for the facial match test as a very small percentage of Lookout match candidates contained valid facial photo images. The results show that the positive facial match accuracy was 62% for the expanded facial match test using a large facial image sample. The results also show that only 25% of false fingerprint matches were found to be positive matches by the secondary facial match process, demonstrating its effectiveness in reducing the overall false matches in the system.

	True Fingerprint Matches	False Fingerprint Matches
Total match pairs used for facial test	42,554	2079
Total matches found to be positive matches by facial match process	26,176	527
Positive facial match %	62%	25%

Table 4: Facial match test results for Recidivist match pairs.

The degradation in positive facial match accuracy from 80% in the initial evaluation test (using a small IDENT facial image set test sample) to 62% for the expanded facial match test (using a large operational IDENT facial image sample) is attributed to: (1) the poor quality of some facial images stored in the IDENT system and (2) inability of the facial match algorithms to positively identify poor quality facial images. By comparison the images used in the expanded facial match test are in general of poorer quality than those used in Face Recognition Vendor Test 2002 [11].

The results of the facial match test study show that facial match accuracy is highly dependent on the quality of the facial images present in both the database and search transactions. The current IDENT client workstation application software does not include a facial image quality check function to ensure the capture of acceptable quality images of subjects. The IDENT capture sites generally do not have the necessary lighting environment to facilitate the capture of facial images of enrolled subjects with acceptable quality. Recognizing the poor quality of facial image capture problem inherent in the current IDENT system, the INS has taken the initiative to develop real-time facial image quality evaluation software for eventual use in the IDENT client application.

The intent of automated facial image quality evaluation software (AFQES) module is to automatically and in real-time determine the suitability of the captured facial image for both the manual human verification and the automated facial identification process. AFEQS quality check software analyzes the captured facial image and measures the quality of facial attributes including head size, head crop, brightness, darkness, glare, blur, and pose. AFEQS analyzes the quality score of the facial attributes and returns the overall quality score of the captured facial image. The overall quality score is used by AFEQS application to determine if the captured facial image was of acceptable quality for storage in the IDENT system. The AFQES software also incorporates the centering guidelines specified in the FBI/NIST Best Practice recommendation for the capture of mugshots.

The results of the INS facial recognition technology research study show some merits in using facial match technology as a secondary match process in conjunction with the existing primary fingerprint match process, for enhancing the overall identification accuracy of the IDENT system. However in order for facial match technology to be an effective secondary match technology for use in the IDENT system, the following operational characteristics need to be in place in the system:

- Improved quality of facial images stored for the IDENT records.
- Ensured availability of acceptable quality facial images for all IDENT enrollment records.
- Integration of automated facial image quality check in the IDENT client to ensure the capture of acceptable quality facial images for enrolled records in the IDENT system.
- Provision of proper lighting and background conditions at INS capture sites to facilitate the capture of acceptable quality facial image in the system.

In addition, improvements in facial matching algorithms will lead to greater robustness in facial match process to handle variation in facial images.

4. Conclusion

This paper has presented the current biometric (fingerprint and face) technologies, lessons learned during the investigative analysis performed to ascertain the benefits of using combined fingerprint and facial technologies and recommendations for the use of current available fingerprint and face identification technologies for optimum identification performance for applications using large user population. Both fingerprint and face recognition accuracy will continue be improved with the advance of technologies. Image quality is one of the main factor affects the overall accuracies of both IDENT and IAFIS systems. Unreadable subject's fingerprints sometimes cause poor image acquisition; however, the primary reason is the improper use of capture devices, and it usually can be improved by proper training.

References

[1] R. Clarke, "Human identification in information systems: Management challenges and public policy issues," Information Technology and People, Vol. 7, No. 4, pp.6-37, 1994.

[2] A. Jain, R. Bolle, and S. Pankanti, editors, "Biometrics: Personal Identification in Networked Society," Kluwer Academic Publishers, 1999.

[3] "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability", November 13, 2002.

[4] G. Snedecor and W. Cochran, "Statistical Methods" 8th edition, Iowa State University Press, 1989.

[5] "Image Quality Study (IQS) Final Report," December 7, 2000, Mitretek Systems (for U.S. Department of Justice, Justice Management Division)

[6] Federal Bureau of Investigation, "The Science of Fingerprints: Classification and Uses," Washington DC, 1984.

[7] L. Jain, U. Halici, I. Hayashi, S. Lee, and S. Tsutsui, editors, "Intelligent Biometric Techniques in Fingerprint and Face Recognition," CRC Press, 1999.

[8] J. Daugman, "Biometric Decision Landscapes," Technical Report No. TR482, University of Cambridge Computer Laboratory, 2000.

[9] A. Jain, L. Hong, S. Pankanti, and R. Bolle, "An Identity-Authentication System Using Fingerprint," Proc. of the IEEE, Vol. 85(9), No. 9, pp. 1365-1388.

[10] INS Facial Match Research Study Report, T-107ST59-1, April 9, 2002.

[11] "FRVT 2002: Overview and Summary", by P.J. Phillips, P. Grother, R.J Micheals, D.M. Blackburn, E Tabassi, and J.M. Bone, March 2003.

[12] P. J. Phillips, A. Martin, C. Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems," IEEE Computer, February 2000.