An Overview on Multi-biometric Score-level Fusion
Verification and Identification

Naser Damer, Alexander Opel and Andreas Shahverdyan
Competence Center Identification and Biometrics,
Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany

Keywords: Multi-biometrics, Score-level Fusion, Biometric Identification.

Abstract: Multi-biometrics is the use of multiple biometric recognition sources to provide a more dependable verification or identification decision. Fusion of multi-biometric sources can be performed on different levels, such as the data, feature, or score level. This work presents an overview of the multi-biometric score-level fusion problem, along with the proposed solution in the literature. A discussion is made to provide a comparison between multi-biometric fusion in both scenarios. This discussion aims at providing a clearer view of future developments especially under the identification scenario where many related applications are rapidly growing such as forensics and ubiquitous surveillance.

SCIENCE AND TECHNOLOGY PUBLICATIONS

1 INTRODUCTION

Biometrics is a rapidly growing technology that aims to identify or verify people identities based on their physical or behavioral properties. Multi-biometrics use more than one biometric recognition approach in a unified frame in an effort to solve problems faced by the conventional uni-modal biometrics. The multi-biometric approach aims at improving biometrics by increasing accuracy, and robustness to intra-person variations and to noisy data. It also aims to solve uni-modal biometrics problems with non-universality and vulnerability to spoof attacks.

Information fusion in multi-biometrics is used to build an identification/verification decision based on the information collected from different biometric sources. The fusion can be done on different levels such as data-level, feature-level, score-level, rank-level or decision-level. In this work, score-level fusion will be inspected as it is widely used to integrate different modalities (based on different biometrics, algorithms and manufacturers) through fusion. Score here refers to the comparison score (similarity) between each captured biometric property and a stored reference.

Biometrics recognition technologies are usually developed under one of two scenarios, verification or identification. Biometric verification is the use of biometrics information to verify a persons claimed identity. Identification, on the other hand, can be defined as the process of assigning a previously registered identity to a person based on the captured biometrics information of the person.

The different nature between verification and identification scenarios effects the implementation of multi-modal biometrics solutions, especially the fusion process. This is due to the different available information in both scenarios, as well as, the different nature of the expected fusion decision.

Figure 1 presents an overview of multi-biometric score-level fusion. Scores from different sources (algorithms and modalities) are normalized then passed into a fusion algorithm. The fusion then results in a fused score.

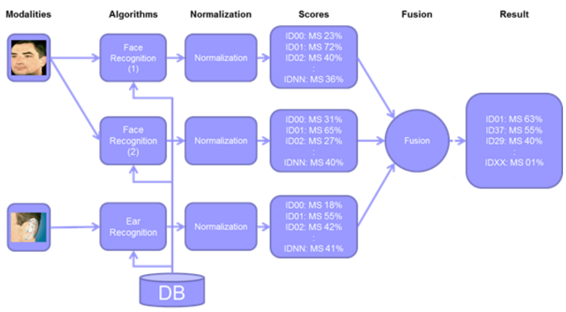

Figure 1: General structure of multi-biometric score-level fusion (Identification). Comparison results are produced by different algorithms and modalities then processed by the normalization stage. The sets of normalized scores feed the fusion algorithm to produce a final set ranked by fused comparison scores.

Damer N., Opel A. and Shahverdyan A..
An Overview on Multi-biometric Score-level Fusion - Verification and Identification.
DOI: 10.5220/0004358306470653
In *Proceedings of the 2nd International Conference on Pattern Recognition Applications and Methods* (BTSA-2013), pages 647-653
ISBN: 978-989-8565-41-9
Copyright © 2013 SCITEPRESS (Science and Technology Publications, Lda.)

In Section 2 below, a literature review is presented covering some of the most interesting works dealing with multi-biometric fusion under both the verification and identification scenarios. The literature review is presented along with the explanation of the different steps of the multi-biometric score-level fusion process. In Section 3, the fusion process under the two scenarios is discussed. A comparison between the natures of the fusion process under both scenarios is also presented. Finally, in Section 4, conclusions and recommendations are drawn.

2 LITERATURE SURVEY

In the following, topics relating to different stages of the multi-biometric fusion process are discussed and connected to cutting edge literature. The topics covered are multi-biometrics schemes, score normalization, fusion algorithms, identification and verification scenarios, consideration of biometric sample quality, available datasets, and finally the robustness to possibly missed data.

2.1 Multi-biometrics

Multi-biometrics is categorized into several approaches depending on the source of multi-decisions from which a unified final decision is built on. The main approaches are multi-modalities, multi-algorithmic, multi-instance, multi-sensorial, and multi-presentation.

Multi-modalities is the use of more than one biometric characteristic as an identity measure. Some works combined fingerprints and face images (K. Nandakumar and Ross, 2009; Tong et al., 2010; Kim et al., 2010), others fused fingerprints and iris biometrics (Baig et al., 2009). Using face images along with iris biometrics was also introduced (Wang et al., 2003). One of the most interesting multi-modal approaches is the use of ear and face biometrics, as they can be easily and non-intrusively captured using same or similar devices (Chang et al., 2003; Yan, 2006). Many other combinations were also introduced, such as ear and fingerprint biometrics (Rattani et al., 2006).

Many works dealt with multi-algorithmic biometrics, such as using multiple face matchers (K. Nandakumar and Ross, 2009; Basak et al., 2010; Kim et al., 2010), or ear identifiers (Moreno et al., 1999; Yan and Bowyer, 2005). Multi-instance fusion was also studied, such as two different fingerprints (Yan and Bowyer, 2005; Basak et al., 2010; Kim et al., 2010), multi-sensorial (Arandjelovic and Hammoud, 2006), and multi-presentation biometric fusion (Cheng et al., 2011) were also discussed thoroughly in the literature.

2.2 Score Normalization

The scores processed by the fusion algorithm are usually not homogeneous as they are produced by different sources. Those scores have to be brought into a common comparable range by a normalization process. Some of the most common normalization techniques are min-max normalization, z-score normalization, double sigmoid, tanh-estimator, and median absolute normalization. The parameters that rule the normalization process are determined based on the statistical properties of the training data. The performances of normalization techniques are not directly comparable as they depend on the overall multi-biometric system.

Here, presented in more details are four of those normalization techniques. The min-max normalization, the z-score, the median absolute deviation (MAD), and the double sigmoid function normalization.

Given comparison scores set S_k, $k = 1,2,\ldots,N$ the normalized score is a function of the score $f(S)$. The min-max normalization depends on the range that the scores span regardless of the distribution properties and aims to map the scores into a range of [0,1]. This normalization scheme was used successfully by many works dealing with score-level multi-biometric fusion (Nisha Srinivas, 2009; Vajaria et al., 2007). The normalized score by min-max normalization is given by:

$$f(S) = \frac{S - min\{S_k\}}{max\{S_k\} - min\{S_k\}}$$

The min-max normalization scheme is highly sensitive to outliers (Jain et al., 2005) as it depends on single minimum and maximum values.

Z-score normalization is a more sophisticated score normalization method and was used in several works (Nisha Srinivas, 2009; Vajaria et al., 2007). Here, the arithmetic mean (μ) and the standard deviation (σ) of the score values are considered. The normalized score by z-score normalization is given by:

$$f(S) = \frac{S - \mu}{\sigma}$$

This method assumes a Gaussian distribution of the score values. This normalization method has low robustness as well, as the parameters μ and σ are sensitive to outliers.

The median absolute deviation normalization method is similar to the z-score normalization method but uses the median and median absolute deviation instead of the mean and standard deviation. This method is more robust to outliers but it also assumes a near Gaussian distribution of the comparison score values. The median absolute deviation normalization is given by:

$$f(S) = \frac{(S - median)}{MAD}$$
$$MAD = median(|\{S_k\} - median)$$

The double sigmoid function is another normalization method. This normalization maps the scores into a range of [0,1] and requires fine tuning of its parameters. The normalization is given by:

$$f(S) = \begin{cases} \frac{1}{1+e^{(-2((S-t)/r_1))}} & if S < t \\ \frac{1}{1+e^{(-2((S-t)/r_2))}} & otherwise. \end{cases}$$

The double sigmoid normalization was used to combine finger print comparison scores by Cappelli et al. (Cappelli et al., 2000).

Marsico et al. recently proposed a novel normalization approach named the Quasi-Linear Sigmoid (QLS) (De Marsico et al., 2011). This approach aims at overcoming the limitations of the traditional normalization algorithms.

The selection of a proper normalization method is a tradeoff between efficiency and robustness, and it depends largely on the nature of the application. Methods like min-max normalization and z-score normalization tend to be more efficient. On the other hand, median absolute deviation normalization and double sigmoid function normalization are usually more robust but require higher computational effort (Jain et al., 2005).

2.3 Fusion Algorithms

Fusion algorithms can be categorized into two main types, combination rules and classification based fusion.

Combination rules are simple operations performed on the normalized scores. Those rules produce a combined score and a classification decision is made based on this combined score value. Main combination rules are the sum rule, weighted sum rule, product rule, max rule, min rule and median rule. Assuming the combined score is a function of the N biometric scores S inputs and is given by $C(S)$. The combination rules can be formulated as follows:

The sum rule: $C(S) = \sum_{i=1}^{N} S_i$

The weighted sum rule: $C(S) = \sum_{i=1}^{N} w_i S_i$, where w_i is the i_{th} weight factor.

The product rule: $C(S) = \prod_{i=1}^{N} S_i$

The max rule: $C(S) = max_i S_i$

The min rule: $C(S) = min_i S_i$

The median rule: $C(S) = median_i S_i$

Some works discussed the difference in performance between the combination rules. Most studies showed the superiority of sum and product combination rules (Hariri and Shokouhi, 2012; Nandakumar et al., 2006; Chang et al., 2004). One must keep in mind that different combination of sum rules and normalization techniques produce different results (L. Latha, 2011).

Classification based fusion considers the input score values as a feature vector. Given those vectors, a classifier is trained to classify a new given vector into genuine or imposter class. Different types of classifiers can be used, just as neural networks (Alsaade, 2010), K-NN (Jin et al., 2004), SVM (Singh et al., 2007; Garcia-salicetti et al., 2005), Adaboost (Ichino et al., 2010; Moin and Parviz, 2009), or as likelihood ratio (Nandakumar et al., 2008; Islam and Rahman, 2010) classifiers. Some works showed comparable results between combination rules and classification based fusion (Rodríguez et al., 2008; Mehrotra et al., 2012). Other works showed the superiority of combination rules (Singh et al., 2007).

2.4 Identification and Verification

Verification is to confirm or reject a claimed identity of a person based on his/her biometric characteristics. Identification is to assign a pre-registered identity to an unknown (no identity claim) person based on his/her biometric characteristics.

The identification process itself can be divided into two different operations, the open-set identification and the closed-set identification. The closed-set identification refers to the situation where the unidentified individual is known to be enrolled in the biometrics reference database. Here, the identification process assigns an ID to the unknown captured individual.

The open-set identification (watchlist) refers to the scenario where the unidentified individual is not definitely enrolled in the biometrics reference database. This case requires verifying the existence of the individual record in the reference database, as well as identifying the individual.

Most of the works dealing with multi-biometrics fusion consider the case of verification (Rodríguez et al., 2008; Jin et al., 2004; Poh and Kittler, 2008; Nisha Srinivas, 2009). Nonetheless, some of the recent works dealt explicitly with the fusion problem under the identification scenario (Basak et al., 2010; K. Nandakumar and Ross, 2009).

A detailed discussion about the differences and interactions between the verification and identification scenarios is presented in Section 3.

2.5 Biometric Sample Quality and Missing Data

In order to compensate for missing information when moving from feature-level fusion to score-level fusion and therefore improve accuracy, the quality of the biometric samples is considered. Beside accuracy, robustness of the biometric system is important. In practice, some of the comparison scores can be missing because of a missing modality or a low quality capture. To build a robust multi-biometric system, the possibility of missing score values must be considered and dealt with so that a reliable biometric decision is made.

2.5.1 Biometric Sample Quality

The quality of the captured biometric sample (image or scan) has an effect on the comparison score values and the confidence of those values as the features extracted from those samples are not reliable (Nandakumar et al., 2006). This reflects on the role a certain score value plays in the fusion process and therefore, taking the quality measures into account will enhance the performance of the fused multi-biometric system (Nandakumar et al., 2006; Poh and Kittler, 2008; Poh et al., 2009).

Nandakumar et al. (Nandakumar et al., 2006) proposed a fusion algorithm that takes into account the sample quality into their likelihood ratio-based fusion scheme. Their experiments proved a highly positive impact of considering the quality measures.

Poh et al. (Poh et al., 2009) proposed a classifier based fusion algorithm that considers the biometric sample quality, as well as, the biometric capture device information. Their experiments clearly showed the effect of including the quality measures on performance.

2.5.2 Missing Data

Multi-biometric systems make a decision based on a set of scores. A case where one or more of those score values are missing may occur, especially in large scale identification systems. Missing data can occur because of the non-universality of a certain biometric modality, or a poorly captured modality in uncontrolled and ubiquitous biometric systems.

Many works considered the problem of missing data and proposed solutions for robust fusion algorithms (Poh et al., 2010b; K. Nandakumar and Ross, 2009; Dinerstein et al., 2007). However, most of those works dealt with the fusion problem under the verification scenario.

Nandakumar et al. proposed a robust fusion solution for multi-biometric fusion under the identification scenario that aims to produce an identification decision regardless of the partially missing data (K. Nandakumar and Ross, 2009). The authors extended the likelihood ratio-based score fusion (originally designed for verification problems) to perform under the identification scenario.

2.6 Databases

In order to build and evaluate an optimized multi-biometric fusion system, a diverse and informative dataset must be available. In this case, a database that contains matching scores from multi-biometrics resources for imposters and genuine matches is required. In the following, four publicly available databases are considered.

The XM2VTS Score-level Fusion Benchmark Dataset (Poh and Bengio, 2006) that contains a database of scores taken from experiments carried out on the XM2VTS face and speaker verification database. Another database is the BANCA score database, a free database that contains 1186 baseline face and speech experiments (Poh,).

Another multi-biometric database was released as a part of the Multiple Biometrics Grand Challenge (Phillips et al., 2009). This database includes face and iris biometric information and aims at the evaluation and improvement of face and iris biometrics captured under uncontrolled conditions.

The Biosecure DS2 database (Poh et al., 2010a) contains biometric comparison scores, as well as the quality measures of the captured biometric samples. The Biosecure DS2 database is considered to be the one of the first databases to build a quality-based fusion benchmark.

3 VERIFICATION VS. IDENTIFICATION

In this section, a comparison between the fusion processes of multi-biometrics under both scenarios is delivered. This comparison will focus on the available information for the fusion algorithm under different scenarios. The expected fusion decision is also discussed. The importance of dealing with image quality and flexibility to missing data is also discussed in this section along with the evaluation measure for the identification and verification problems.

3.1 Available Information

The verification process starts by supplying the biometric system with a claimed identity and one or more captured biometrics characteristics. The claimed identity has one or more corresponding biometrics references stored in a dataset. The biometric verification system matches the captured biometrics with the corresponding stored biometric reference. In a sum, the available information in the verification scenario is the claimed identity, captured biometrics of the subject and the corresponding biometrics references of the claimed subject. Those information leads to only one set (belongs to one identity) of biometrics comparison scores to be fed into the fusion algorithm.

Identification aims to compare the subject's captured biometric characteristics with the available references in the dataset to build an identification decision. Therefore, the available information are the captured biometrics of the subject and the references of all the enrolled subjects. This leads to a number of comparison scores sets. This number can be equal to the number of enrolled subjects or a subset of them (if initial guess was made). Those sets of comparison scores are then fed into the fusion algorithm to build the identification decision.

While building the fusion algorithm, the information available for both identification and verification scenarios are similar. As the identities are known while training, one can get access to the comparison scores between all captured biometrics and all references. Therefore, a set of genuine/imposter comparison scores is available to help optimize the fusion algorithm in both scenarios. However, the availability of multiple comparisons in the identification scenario can provide more information about the genuinity of a certain capture. It is expected that a larger difference between the first and second ranked matches indicates a higher confidence that the first rank is the genuine match. This kind of information is only available under the identification scenario.

3.2 Expected Decision

The expected output of the fusion algorithm varies between verification and identification scenarios. Given the set of comparison scores between the captured biometrics and the references of the claimed identity, the verification process output is a binary decision. This decision marks the claimed identity either as genuine (true) or imposter (false).

In identification, given the sets of biometrics comparison scores between the captured subject and all stored references (sometimes partial set), the fusion decision must rank the stored identities by similarity to the captured subject.

It must be mentioned that open-set identification operation must be followed by a verification process for the top ranked identity. This verification ensures that the top ranked identity is the correct identity. Especially when the database may not include the identity of interest. If the verification of the top ranked identity resulted in an imposter decision, the captured person is believed not to be registered in the reference database.

3.3 Quality Measures, Missed Data and Evaluation

The accuracy of the fusion decision largely depends on the quality of the comparison processes of the different modalities. This quality of the comparison in each modality depends on different factors. It is affected by the quality of the captured biometric information, the quality of the stored biometric reference and the quality of the capturing device itself. It is also dependent on the quality of the comparison algorithm and the features used to represent the biometrics. The accuracy of the fusion algorithm is also affected by the quality of the preprocessing of comparison scores i.e. normalization.

The biometric decision in verification is based only on one set of captured biometrics and one set (ID) of references (1:1 match). However, under identification, the decision is based on more than one set of biometric references (1:N match). This fact leads to the believe that the identification scenario is more affected by the quality measures, especially in the cases where the quality of biometrics references vary largely.

One of the main reasons to use multi-modal biometrics is the pursuit of higher robustness in biometric systems. This appears usually when considering the universality of biometric systems, as well as designing ubiquitous biometric systems. Multi-modal biometric systems must be designed to be functional even when some information are missed, this directly affect the fusion algorithm design and have different effects under the verification and identification scenarios.

A missing biometric measure in a verification scenario can occur because of a missed captured biometric characteristic or a missed reference within the claimed identity references set. In identification, a missed captured biometric measure, as well as a missed reference can occur. However, under identification where the system depends on a large number of references sets, the missed modality can be different in each comparison between each ID pair. This situation argues the development of more advanced and flexible solutions for missing data under the identification scenario.

The performance evaluation of a multi-biometric systems is not different than that of a conventional uni-modal biometric systems. Identification results are usually represented in a Cumulative Match Characteristic (CMC) curve, especially when dealing with closed-set identification. The verification performance is shown usually as Receiver Operating Characteristic (ROC) curve and as an equal error rate (EER).

4 CONCLUSIONS

This work presented an overview on the score-level multi-biometric fusion problem. Some of the most interesting works in this field were discussed along with the structured steps of the multi-biometric fusion process. A comparison between the multi-biometric systems under identification and verification scenarios was drawn. The discussion presented aims at providing a clear view on multi-biometric system development especially under the relatively understudied identification scenario.

ACKNOWLEDGEMENTS

This work is funded by the Federal Ministry of Education and Research (BMBF) of Germany in the context of the research programme for public safety and security.

REFERENCES

Alsaade, F. (2010). A study of neural network and its properties of training and adaptability in enhancing accuracy in a multimodal biometrics scenario. *Information Technology Journal*.

Arandjelovic, O. and Hammoud, R. (2006). Multi-sensory face biometric fusion (for personal identification). In *Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop*, CVPRW '06, pages 128–, Washington, DC, USA. IEEE Computer Society.

Baig, A., Bouridane, A., Kurugollu, F., and Qu, G. (2009). Fingerprint - iris fusion based identification system using a single hamming distance matcher. In *Proceedings of the 2009 Symposium on Bio-inspired Learning and Intelligent Systems for Security*, BLISS '09, pages 9–12, Washington, DC, USA. IEEE Computer Society.

Basak, J., Kate, K., Tyagi, V., and Ratha, N. (2010). A gradient descent approach for multi-modal biometric identification. In *Pattern Recognition (ICPR), 2010 20th International Conference on*, pages 1322 –1325.

Cappelli, R., Maio, D., and Maltoni, D. (2000). Combining fingerprint classifiers. In *Proceedings of the First International Workshop on Multiple Classifier Systems*, MCS '00, pages 351–361, London, UK, UK. Springer-Verlag.

Chang, K., Bowyer, K. W., Sarkar, S., and Victor, B. (2003). Comparison and combination of ear and face images in appearance-based biometrics. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 25:1160–1165.

Chang, K. I., Bowyer, K. W., Flynn, P. J., and Chen, X. (2004). Multi-biometrics using facial appearance, shape and temperature. In *Proceedings of the Sixth IEEE international conference on Automatic face and gesture recognition*, FGR' 04, pages 43–48, Washington, DC, USA. IEEE Computer Society.

Cheng, X., Tulyakov, S., and Govindaraju, V. (2011). Multiple-sample fusion of matching scores in biometric systems. In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2011 IEEE Computer Society Conference on*, pages 120 –125.

De Marsico, M., Nappi, M., Riccio, D., and Tortora, G. (2011). Nabs: Novel approaches for biometric systems. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 41(4):481 –493.

Dinerstein, S., Dinerstein, J., and Ventura, D. (2007). Robust multi-modal biometric fusion via multiple svms. In *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Montral, Canada, 7-10 October 2007*, pages 1530–1535. IEEE.

Garcia-salicetti, S., Mellakh, M. A., Allano, L., and Dorizzi, B. (2005). Multimodal biometric score fusion: The mean rule vs. support vector classifiers. In *Proceedings of the EUSIPCO*.

Hariri, M. and Shokouhi, S. B. (2012). Robustness of multi biometric authentication systems against spoofing. *Computer and Information Science*, pages 77–86.

Ichino, M., Komatsu, N., Wang, J.-G., and You, W. Y. (2010). Speaker gender recognition using score level fusion by adaboost. In *11th International Conference on Control, Automation, Robotics and Vision, ICARCV 2010, Singapore, 7-10 December 2010, Proceedings*, pages 648–653. IEEE.

Islam, M. R. and Rahman, M. F. (2010). Article:likelihood ratio based score fusion for audio-visual speaker identification in challenging environment. *International Journal of Computer Applications*, 6(7):6–11. Published By Foundation of Computer Science.

Jain, A., Nandakumar, K., and Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern Recogn.*, 38(12):2270–2285.

Jin, A. T. B., Samad, S. A., and Hussain, A. (2004). Nearest neighbourhood classifiers in a bimodal biometric verification system fusion decision scheme. *Journal of Research and Practice in Information Technology*, 36(1):47–62.

K. Nandakumar, A. K. J. and Ross, A. (2009). Fusion in multibiometric identification systems: What about the missing data? In *Proceedings of the 3rd International Conference on Biometrics, Alghero, Italy*.

Kim, Y., Toh, K.-A., and Teoh, A. (2010). An online learning algorithm for biometric scores fusion. In *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on*, pages 1 –6.

L. Latha, S. T. (2011). On improving the performance of multimodal biometric authentication through ant colony optimization. *WSEAS Transactions on Information Science and Applications*.

Mehrotra, H., Vatsa, M., Singh, R., and Majhi, B. (2012). Biometric match score fusion using rvm: A case study in multi-unit iris recognition. In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2012 IEEE Computer Society Conference on*, pages 65 –70.

Moin, M. S. and Parviz, M. (2009). Exploring auc boosting approach in multimodal biometrics score level fusion. In *Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IIH-MSP '09, pages 616–619, Washington, DC, USA. IEEE Computer Society.

Moreno, B., Sanchez, A., and Velez, J. (1999). On the use of outer ear images for personal identification in security applications. In *Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on*, pages 469 –476.

Nandakumar, K., Chen, Y., Dass, S. C., and Jain, A. (2008). Likelihood ratio-based biometric score fusion. *IEEE Trans. Pattern Anal. Mach. Intell.*, 30(2):342–347.

Nandakumar, K., Chen, Y., Jain, A. K., and Dass, S. C. (2006). Quality-based score level fusion in multibiometric systems. In *Proceedings of the 18th International Conference on Pattern Recognition - Volume 04*, ICPR '06, pages 473–476, Washington, DC, USA. IEEE Computer Society.

Nisha Srinivas, Kalyan Veeramachaneni, L. O. (2009). Fusing correlated data from multiple classifiers for improved biometric verification. In *12th International Conference on Information Fusion*.

Phillips, P., Flynn, P., Beveridge, J., Scruggs, W., OToole, A., Bolme, D., Bowyer, K., Draper, B., Givens, G., Lui, Y., Sahibzada, H., Scallan, JosephA., I., and Weimer, S. (2009). Overview of the multiple biometrics grand challenge. In Tistarelli, M. and Nixon, M., editors, *Advances in Biometrics*, volume 5558 of *Lecture Notes in Computer Science*, pages 705–714. Springer Berlin Heidelberg.

Poh, N. Banca score database.

Poh, N. and Bengio, S. (2006). Database, protocols and tools for evaluating score-level fusion algorithms in biometric authentication. *Pattern Recogn.*, 39(2):223–233.

Poh, N., Bourlai, T., and Kittler, J. (2010a). A multimodal biometric test bed for quality-dependent, cost-sensitive and client-specific score-level fusion algorithms. *Pattern Recogn.*, 43(3):1094–1105.

Poh, N. and Kittler, J. (2008). A family of methods for quality-based multimodal biometric fusion using generative classifiers. In *ICARCV*, pages 1162–1167. IEEE.

Poh, N., Merati, A., and Kittler, J. (2009). Making better biometric decisions with quality and cohort information: A case study in fingerprint verification. In *Proc. 17th European Signal Processing Conf. (Eusipco)*, pages 70–74, Glasgow.

Poh, N., Windridge, D., Mottl, V., Tatarchuk, A., and Eliseyev, A. (2010b). Addressing missing values in kernel-based multimodal biometric fusion using neutral point substitution. *Trans. Info. For. Sec.*, 5(3):461–469.

Rattani, A., Kisku, D. R., Bicego, M., and Tistarelli, M. (2006). Robust Feature-Level Multibiometric Classification. *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the*, pages 1–6.

Rodríguez, L. P., Crespo, A. G., Lara, M. J. P., and Mezcua, B. R. (2008). Study of different fusion techniques for multimodal biometric authentication. In *Proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication*, WIMOB '08, pages 666–671, Washington, DC, USA. IEEE Computer Society.

Singh, R., Vatsa, M., and Noore, A. (2007). Intelligent biometric information fusion using support vector machine. In Nachtegael, M., Van der Weken, D., Kerre, E., and Philips, W., editors, *Soft Computing in Image Processing*, volume 210 of *Studies in Fuzziness and Soft Computing*, pages 325–349. Springer Berlin Heidelberg.

Tong, Y., Wheeler, F., and Liu, X. (2010). Improving biometric identification through quality-based face and fingerprint biometric fusion. In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2010 IEEE Computer Society Conference on*, pages 53 –60.

Vajaria, H., Islam, T., Mohanty, P., Sarkar, S., Sankar, R., and Kasturi, R. (2007). Evaluation and analysis of a face and voice outdoor multi-biometric system. *Pattern Recogn. Lett.*, 28(12):1572–1580.

Wang, Y., Tan, T., and Jain, A. (2003). Combining face and iris biometrics for identity verification. In Kittler, J. and Nixon, M., editors, *Audio- and Video-Based Biometric Person Authentication*, volume 2688 of *Lecture Notes in Computer Science*, pages 805–813. Springer Berlin Heidelberg.

Yan, P. (2006). *Ear biometrics in human identification*. PhD thesis, University of Notre Dame, Notre Dame, IN, USA. AAI3406950.

Yan, P. and Bowyer, K. W. (2005). Multi-biometrics 2d and 3d ear recognition. In Kanade, T., Jain, A. K., and Ratha, N. K., editors, *AVBPA*, volume 3546 of *Lecture Notes in Computer Science*, pages 503–512. Springer.

SCIENCE AND TECHNOLOGY PUBLICATIONS