Mayank Vatsa, Richa Singh, Afzel Noore
Lane Department of Computer Science and Electrical Engineering,
West Virginia University, U.S.A.
{mayankv, richas, noore}@csee.wvu.edu

Framework for biometric match score fusion using statistical and belief models

Published in:
Florentin Smarandache & Jean Dezert (Editors)
Advances and Applications of DSmT for Information Fusion
(Collected works), Vol. III
American Research Press (ARP), Rehoboth, 2009
ISBN-10: 1-59973-073-1
ISBN-13: 978-1-59973-073-8
Chapter XVII, pp. 455 - 469

Abstract: *This chapter presents a framework for multi-biometric match score fusion when non-ideal conditions cause conflict in the results of different unimodal biometrics classifiers. The proposed framework uses belief function theory to effectively fuse the match scores and density estimation technique to compute the belief assignments. Fusion is performed using belief models such as Transferable Belief Model and Proportional Conflict Redistribution rule followed by the likelihood ratio based decision making. Two case studies on multiclassifier face verification and multiclassifier fingerprint verification show that the proposed fusion framework with PCR5 rule yields the best verification accuracy even when individual biometric classifiers provide conflicting match scores.*

17.1 Introduction

The performance of the biometric recognition algorithms depends on several factors such as biometric modality, application environment, and database. For example, the performance of fingerprint recognition algorithms depend on the quality of fingerprint to be recognized, the resolution and the type of the fingerprint sensor, and the number of features present in the image. The face recognition algorithms require good quality images with representative training database. Signature biometrics depend on the type of pen and mode of capture. Variation in any of these factors often lead to poor verification performance. To overcome this problem, researchers have proposed the use of multi-biometrics for recognition. Multi-biometrics combines two or more biometric modalities and it has been established that fusion of multiple biometric evidences enhances the recognition performance [12, 19]. Biometric fusion can be performed at data level, at feature level, at match score level, at decision level, or at rank level. Data level fusion combines raw biometric data such as infrared and visible face images. Feature level fusion combines multiple features extracted from the individual biometric data to generate a new feature vector which is subsequently used for recognition. In match score fusion, the features extracted from individual biometric are first matched to compute the corresponding match scores which are then combined to generate a fused match score. In decision level fusion, decisions of individual biometric classifiers are fused to compute a combined decision. Rank level fusion involves combining identification ranks obtained from multiple unimodal identification systems. Further, multi-biometrics can be a multiclassifier system, a multi-unit system, or a multimodal system. In multiclassifier systems, different classifiers are used to extract different types of features to perform matching and fusion. For example, in face biometrics, global and local facial features can be extracted using different classifiers/algorithms and then information can be fused. In multi-unit system, multiple samples of the same biometrics are used for feature extraction and fusion. For example, texture features can be extracted for both left and right iris images and then information from these images are combined. In multimodal system, information from two or more modalities are combined, e.g. face-fingerprint bimodal system.

In this research, we focus on match score fusion to enhance the performance of biometric systems. Existing biometric match score fusion algorithms can be divided into three categories: statistical fusion algorithms, learning based fusion algorithms, and belief function theory based fusion algorithms. Statistical fusion algorithms are based on statistical rules such as AND rule, OR rule, and SUM rule [15]. Learning based fusion algorithms use learning techniques such as support vector machine and neural network to train the fusion algorithm and then use the trained model to decide whether an individual is genuine or an impostor [2]. Belief function theory based fusion algorithms [18, 21] use the match scores to compute the belief assignments and then combine them. Existing evidence based fusion algorithms use Dempster Shafer (DS) theory [16, 33] and Dezert Smarandache (DSm) theory [5, 6] in which match scores are considered as evidence over a frame of discernment.

A major problem with statistical and learning based multi-biometric fusion algorithms occurs when different biometric classifiers generate highly conflicting results for the same individual. Specifically, if one classifier strongly supports one hypothesis and the other classifier strongly rejects the same hypothesis. For example, in a face and fingerprint based bimodal biometric system, variance in image capture, image quality, lighting conditions, facial expressions, and sensor noise could generate a face match score of 0.8 (perfect accept is 1) and a fingerprint match score of 0.2 (perfect reject is 0). Existing fusion algorithms may not be able to handle such conflicting information and degrade the performance drastically. Further, belief function theory based fusion algorithms are computationally expensive. To address these issues and improve the verification performance of a biometric system, we propose a framework for multi-biometric fusion which combines the belief function theory with statistical methods. Further, density estimation technique is used for computing the belief models such as DS theory, Transferable Belief Model (TBM) [23, 25], DSm fusion, and Proportional Conflict Redistribution (PCR) rule [6] for information fusion, and likelihood ratio for decision making.

Section 17.2 briefly presents the fundamental concepts and notations involved in the belief function theory based fusion algorithms. Section 17.3 describes the proposed biometric match score fusion framework and Section 17.4 describes the algorithms and databases used for evaluation. Sections 17.5 discuss the experimental results of the proposed fusion framework. Section 17.6 briefly presents the concept of a biometric unification framework.

17.2 Overview of belief function theory based fusion algorithms

Belief function theory or the theory of evidence is a theoretical framework for reasoning with imperfect data. It is a generalization of probability theory and includes many approaches of reasoning under uncertainty. Examples of such approaches are Dempster Shafer theory, Transferable Belief Model, Dezert Smarandache fusion, and Proportional Conflict Redistribution rule. In this section, only the main concepts and notations of DS theory, TBM, DSm fusion, and PCR rule are presented for a two class - two classifier problem. A detailed explanation of belief function theory can be found in [16, 31].

Let $m \in [0, 1]$ be a mapping function and $\Theta = \{\theta_1, \theta_2\}$ be the frame of discernment that represents the finite set of exhaustive and mutually exclusive hypothesis. Probability theory, as mentioned before, is the basis of belief function theory. Belief function, also known as the basic probability assignment, (*bpa*) is defined as $m(\cdot) : \Theta \rightarrow [0, 1]$, such that $m(\theta_1) + m(\theta_2) = 1$. Here, $m(\theta_1)$ represents the belief of data belonging to class θ_1 and $m(\theta_2)$ represents the belief of data belonging to θ_2.

In the probabilistic framework, basic fusion rule is sum rule as defined in Equations (17.1) and (17.2) (for two information sources).

$$m_{fused}(\theta_1) = \frac{m_1(\theta_1) + m_2(\theta_1)}{2} \tag{17.1}$$

$$m_{fused}(\theta_2) = \frac{m_1(\theta_2) + m_2(\theta_2)}{2} \tag{17.2}$$

The basic sum rule fusion, though effective for simple non-conflicting cases, is not very effective for imprecise, uncertain, and conflicting cases. To address the limitations of the sum rule, approximate reasoning approach based fusion rules including DS theory, TBM and DSm fusion have been proposed. In DS theory, belief functions have been computed on the power set of Θ (i.e. 2^{Θ}) and Dempster's rule of combination [16, 33] for fusing two information sources, X and Y, is defined as,

$$m_{DS}(A) = \frac{\sum_{(X,\, Y \in 2^{\Theta}),(X \cap Y = A)} \; m(X)m(Y)}{1 - \sum_{(X,\, Y \in 2^{\Theta}),(X \cap Y = \emptyset)} \; m(X)m(Y)} \tag{17.3}$$

Although DS theory based fusion has been efficiently used for many practical applications, it has some limitations. As presented by Zadeh [34], Dubois and Prade [7], Voorbraak [31], and Dezert and Smarandache [6], DS theory is not reliable when conflict between the sources is very large. To circumvent the limitations of DS fusion algorithm, researchers have proposed several other models. Smets proposed the transferable belief model [23] that quantitatively represents the epistemic uncertainty. According to Smets, the TBM conjunctive combination rule for fusing two information sources, X and Y, can be represented as,

$$m_{TBM}(A) = \sum_{X,\, Y \in 2^{\Theta}} m(X)m(Y) \tag{17.4}$$

Recently, Dezert and Smarandache proposed a fusion algorithm using plausible and paradoxical reasoning [6] that addresses the limitations of DS theory and includes Bayes theory and DS theory as special cases. It operates on the hyper-power set defined as $D^{\Theta} = \{\emptyset, \theta_1, \theta_2, \theta_1 \cup \theta_2, \theta_1 \cap \theta_2\}$. This algorithm uses generalized basic belief assignment (gbba) on Θ which is defined as $m(\cdot) : D^{\Theta} \rightarrow [0, 1]$ such that

$$\begin{aligned} &m(\emptyset) = 0 \\ &m(\theta_1) + m(\theta_2) + m(\theta_1 \cup \theta_2) + m(\theta_1 \cap \theta_2) = 1 \end{aligned} \tag{17.5}$$

For fusing two information sources, X and Y, the DSm rule of combination [5] is defined as,

$$m_{\mathcal{M}(\Theta)}(A) = \psi(A)\left[S_1(A) + S_2(A) + S_3(A)\right] \tag{17.6}$$

where, $\mathcal{M}(\Theta)$ is the model over which DSm theory operates and $\psi(A)$ is the characteristic non-emptiness function of A which is 1 if $A \notin \emptyset$ and 0 otherwise. $S_1(A)$, $S_2(A)$, and $S_3(A)$ are defined as,

$$\begin{array}{lll} S_1(A) = & \sum_{(X,Y\in D^\Theta,\ X\cap Y=A)} & m_1(X)\, m_2(Y) \\ S_2(A) = & \sum_{(X,Y\in \mathbf{\Phi},\ [\upsilon=A]\vee[(\upsilon\in\mathbf{\Phi})\wedge(A=I_t)])} & m_1(X)\, m_2(Y) \\ S_3(A) = & \sum_{(X,Y\in D^\Theta,\ X\cup Y=A,\ X\cap Y\in\mathbf{\Phi})} & m_1(X)\, m_2(Y) \end{array} \tag{17.7}$$

where I_t is the total ignorance and is the union of all θ_i $(i = 1, 2)$, i.e. $I_t = \theta_1 \cup \theta_2$. $\mathbf{\Phi} = \{\mathbf{\Phi}, \phi\}$ is the set of all elements of D^Θ which are empty under the constraints of some specific problem and ϕ is the empty set. $\upsilon = u(X) \cup u(Y)$, where $u(X)$ is the union of all singletons θ_i that compose X and Y. Here, $S_1(A)$ corresponds to the classical DSm rule on the free DSm model [5], $S_2(A)$ represents the mass of all relatively and absolutely empty sets which is transferred to the total or relative ignorance, and $S_3(A)$ transfers the sum of relative empty sets to the non-empty sets.

In the DSm fusion algorithm, the partial conflicts are redistributed onto corresponding partial ignorance [5]. However, in some cases this redistribution may yield very non-specific generalized basic belief assignments and thus decrease the performance. Further analysis by Smets [25] suggests that the term S_2 in Equation (17.7) is a "potential source of difficulties" and "seems to be language dependent". To address this issue, Dezert and Smarandache proposed a set of proportional conflict redistribution rules [6] which consists of five different versions of the PCR rule; PCR1 to PCR5 in order of increasing complexity and correctness. They have reported that among the five rules, PCR5 is the most efficient and precise for information fusion under uncertainty and conflict. In PCR5, redistribution of the partial conflicts is performed only to the elements which are truly involved in each partial conflict and moreover this is done according to the proportion or weight of each source. For a two class - two classifier problem and $\forall X \in D^\Theta \setminus \{\emptyset\}$, the PCR5 rule [6] is defined as

$$m_{PCR5}(X) = m_{12}(X) + \sum_{Y\in D^\Theta\setminus\{X\},\ X\cap Y=\emptyset} \left[\frac{m_1(X)^2 m_2(Y)}{m_1(X)+m_2(Y)} + \frac{m_2(X)^2 m_1(Y)}{m_2(X)+m_1(Y)} \right] \tag{17.8}$$

In this equation, m_1 and m_2 represent the corresponding belief assignments to the two classifiers; $m_{12}(X)$ corresponds to the conjunctive consensus on X between the two sources and where all denominators are different from zero. If a denominator is zero, that fraction is discarded. All sets involved in the formula are in canonical form.

The PCR5 fusion rule precisely combines and redistributes the information even with conflicting gbba's. A detailed explanation of the PCR rules can be found in [6].

17.3 Framework for biometric match score fusion

In biometrics, DS theory has been used for match score and decision fusion [4, 18]. However, as mentioned in Section 17.2, DS theory has some limitations and it cannot always provide good results with imprecise, imperfect or uncertain data. In our

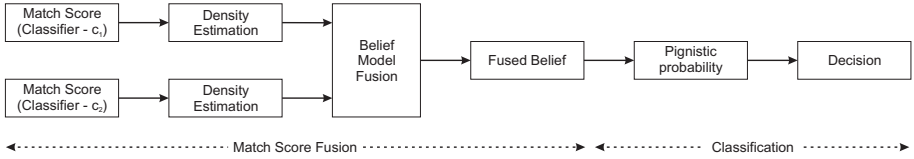

Figure 17.1: Proposed match score fusion framework.

previous research, we proposed the use of DSm theory for biometrics match score fusion [21, 28]. In our experiments, we found that there are few cases when DSm theory is not able to yield correct results and sometimes the decisions are not accurate. As discussed in Section 17.2, sometimes DSm fusion generates non-specific belief assignments which reduce the performance because of the term S_2 in Equation (17.7).

In this chapter, a generalized framework is presented in which the belief theory based fusion approach is combined with the statistical approach. In the proposed framework, the first step is to transform the match scores into belief assignments using density estimation technique. In the next step, a belief theory based algorithm is used for match score fusion and finally a statistical likelihood ratio test is applied for classification. In this manner, the properties of both statistical and belief function theories are combined for biometric match score fusion. Figure 17.1 shows the steps involved in the proposed framework. This fusion framework consists of two steps: (1) match score fusion and (2) classification. In this chapter, the description of the proposed framework uses two class - two classifier approach and the subscript c_1 represents the first biometric classifier and subscript c_2 represents the second biometric classifier.

17.3.1 Match score fusion

Let the frame of discernment $\Theta = \{\theta_{gen}, \theta_{imp}\}$, where θ_{gen} represents the genuine hypothesis and θ_{imp} represents the impostor hypothesis. The first step in the proposed fusion framework is to transform the match scores into belief assignments. We use a density estimation technique for this task assuming that the match scores follow a Gaussian distribution. This method transforms a match score into the probability measure which is helpful in computing belief assignment. Gaussian density estimation [8] can be written as,

$$p(s_i, \mu_{ij}, \sigma_{ij}) = \frac{1}{\sigma_{ij}\sqrt{2\pi}} exp\left[-\frac{1}{2}\left\{\frac{s_i - \mu_{ij}}{\sigma_{ij}}\right\}^2\right] \tag{17.9}$$

where s_i, $(i = 1, 2)$ are the two match scores to be fused, μ_{ij} and σ_{ij} are the mean and standard deviation of the i^{th} classifier corresponding to the j^{th} element of z (in

basic sum rule $z = \Theta$, in DS theory $z = 2^{\Theta}$ and in DSm theory $z = D^{\Theta}$). Therefore the Gaussian distribution is used to compute the belief $m_i(j)$,

$$m_i(j) = \frac{p(s_i, \mu_{ij}, \sigma_{ij})}{\sum_{j=1}^{z} p(s_i, \mu_{ij}, \sigma_{ij})} \tag{17.10}$$

The belief assignments of each biometric classifier are then fused using eq. (17.11)

$$m_{fused} = m_{c1} \oplus m_{c2} \tag{17.11}$$

where $\oplus$ represents the fusion rule described in Section 17.2. Note that, in this research, we evaluate the performance of the proposed fusion framework with the basic sum rule, DS theory fusion, TBM conjunctive combination rule, DSm fusion rule, and PCR rule.

17.3.2 Statistical classification

Match score fusion using the proposed framework yields the fused belief and a decision of *accept* or *reject* is made using the statistical classification technique. First, the fused beliefs are converted into probability measure using the pignistic probability, $BetP$, that maps a belief measure to a probability measure [23].

$$BetP(\theta_i) = \sum_{\theta_i \in A \subseteq \Theta} \frac{1}{|A|} \frac{m_{fused}(A)}{1 - m_{fused}(\emptyset)} \tag{17.12}$$

If $m_{fused}(\emptyset) = 0$, Equation (17.12) can be written as,

$$BetP(\theta_i) = \sum_{\theta_i \in A \subseteq \Theta} \frac{m_{fused}(A)}{|A|} \tag{17.13}$$

In this manner, we transform fused belief assignment into probability measure so that we can apply the statistical classification approach for computing the final decision. We perform likelihood ratio test for decision making as shown in Equation (17.14).

$$Decision = \begin{cases} genuine & if \quad \frac{BetP(\theta_{gen})}{BetP(\theta_{imp})} \geq t \\ impostor & otherwise \end{cases} \tag{17.14}$$

where t is the decision threshold and is chosen based on a specific false accept rate. The advantage of this statistical classification approach is its simplicity, control over false accept and false reject rates, and it satisfies the Neyman-Pearson theorem [13] for decision making.

17.4 Algorithms and databases used for evaluation

To evaluate the verification performance of the proposed fusion framework described in Section 17.3, we use two case studies: (1) multiclassifier face verification and (2) multiclassifier fingerprint verification. In this section, we briefly describe the algorithms and databases used for evaluation.

17.4.1 Face verification algorithms

The first case study for evaluating the performance of the proposed fusion framework is performed with multiclassifier face verification. The face is first detected from the input images using the triangle based face detection algorithm [17]. Global and local facial features are extracted and match scores are computed from the detected face images using the two face verification algorithms described below.

- **2D Log Polar Gabor Transform:** In the 2D log polar Gabor transform based face recognition algorithm, the face image is transformed into polar coordinates and texture features are extracted using the neural network architecture based 2D log polar Gabor transform [20]. These features are matched using Hamming distance to generate the match scores.
- **Local Binary Pattern:** In this algorithm, a face image is divided into several regions and weighted Local Binary Pattern (LBP) features are extracted to generate a feature vector [3]. Matching of two LBP feature vectors is performed using the weighted Chi-square distance measure.

In this case study, the two face classifiers are represented as c_1 and c_2, and the match scores computed using these classifiers are combined using the proposed fusion framework.

17.4.2 Fingerprint verification algorithm

Multiclassifier fingerprint verification is used as the second case study for evaluating the performance of the proposed fusion framework. Level-2 minutiae and level-3 pore features based verification algorithms are used to compute the match scores.

- **Level-2 Minutia Verification Algorithm**: A ridge tracing minutiae extraction algorithm [11] is used to extract the level-2 minutia features from a fingerprint image. Gallery and probe minutiae are matched using a dynamic bounding box based matching algorithm [10].
- **Level-3 Pore and Ridge Verification Algorithm**: The level-3 pore and ridge feature extraction algorithm [29] uses Mumford Shah functional curve evolution based fast feature extraction algorithm to efficiently segment contours and extract the intricate level-3 features. Matching of gallery and probe feature sets is performed using the Mahalonobis distance measure.

These minutiae and pore based matching algorithms are used as classifiers c_1 and c_2 and the corresponding match scores are fused using the proposed fusion framework.

17.4.3 Biometric databases used for evaluation

We use two biometric databases for these case studies. These databases are: Notre Dame face database [1, 9] used for evaluating the performance for multiclassifier face verification and high resolution fingerprint database for the experiments related to multiclassifier fingerprint verification.

1. **Notre Dame Face Database** [9]: This database is a part of the NIST Face Recognition Grand Challenge (FRGC). We use collection B of the Notre Dame face database which contains around 35,000 high resolution frontal face images under different lighting conditions and expressions. It is one of the most comprehensive face databases widely used for evaluating the performance of face recognition algorithms.

2. **High Resolution Fingerprint Database** [28]: The high resolution fingerprint database contains 5500 images from 550 classes. For each class, there are 10 fingerprints. The resolution of fingerprint images is 1000 ppi to facilitate the extraction of both level-2 minutiae and level-3 pore features.

17.5 Experimental evaluation

As mentioned before, the proposed fusion framework is evaluated for two multibiometric scenarios. For each case study, we compute the verification accuracy of the proposed fusion framework with sum rule, DS theory fusion, TBM, DSm and PCR rule. For performance evaluation, we use cross validation with 20 trials. Three images are randomly selected for training (estimating densities, thresholds, and learning classifiers) and the remaining images are used as the test data to evaluate the algorithms. This train-test partitioning is repeated 20 times and the Receiver Operating Characteristics (ROC) curves are generated by computing the genuine accept rates (GAR) over these trials at different false accept rate (FAR). This section presents the experimental results with their analysis.

To evaluate the performance of the proposed fusion framework, we use multiclassifier face verification using the Notre Dame face database as the first case study. The ROC plot in Figure 17.2 and Table 17.1 show the verification accuracies of this case study. Here classifier 1 is the 2D log polar Gabor transform based verification algorithm that yields an average verification accuracy of 93.1% at 0.01% FAR and classifier 2 is the local binary pattern based verification algorithm that yields an average verification accuracy of 82.3% at 0.01% FAR.

The sum rule based fusion algorithm (using bpa) improves the verification performance by 4.6%. During our experiments, we analyze that the Sum rule fusion

Algorithms	Verification Accuracy (%)			
	Multiclassifier Face Verification		Multiclassifier Fingerprint Verification	
	Average	[Max., Min.]	Average	[Max., Min.]
Classifier 1	93.1	[94.3, 85.7]	88.9	[92.1, 83.6]
Classifier 2	82.3	[90.5, 78.1]	91.5	[93.5, 90.8]
Sum Rule	97.7	[98.8, 92.6]	97.1	[98.2, 93.5]
DS Theory Fusion	98.0	[98.9, 95.7]	97.7	[99.0, 95.4]
TBM Fusion Rule	98.2	[99.0, 96.1]	98.2	[99.1, 96.6]
DSm Fusion Rule	98.5	[99.1, 97.3]	98.7	[99.3,98.1]
PCR5 Fusion Rule	**98.9**	**[99.8, 98.2]**	**99.1**	**[99.9, 98.5]**

Table 17.1: Experimental results of fusion algorithms at 0.01% FAR.

algorithm is not able to handle most of the conflicting cases. Furthermore, during different cross validation trials, we also observe that the variance in the verification accuracies obtained by the sum rule is very large. This shows that the Sum rule is not very stable and it depends upon the training images. The proposed fusion framework with DS fusion, TBM, and DSm fusion improves the verification accuracy in the range of 4.9-5.4% and is more stable compared to the Sum rule. Analysis of the experimental results of the proposed fusion framework with DS fusion, TBM rule, and DSm fusion show that the these three rules efficiently redistribute the beliefs and fuse the match scores which are not highly conflicting. However, with highly conflicting match scores that are caused due to variations in expression, lighting and time difference between gallery and probe face images, they do not provide reliable decision. The proposed framework with PCR5 rule yields the best verification accuracy of 98.9%. This is because the fusion framework with PCR5 rule first performs efficient redistribution of the partial conflicts according to the proportion/weight of each source. After redistribution, the belief measure is transformed into the probability measure and likelihood ratio test is used for decision. In this manner, it includes the properties of the theory of evidence and satisfies the Neyman-Pearson theorem [13] as well. Finally, the proposed framework with PCR5 fusion is the most stable algorithm across all cross validation trials whereas verification accuracies pertaining to other fusion algorithms vary significantly.

The second case study on multiclassifier fingerprint verification shows similar results. The ROC plot in Figure 17.3 and Table 17.1 show the verification accuracies of this case study. Level-2 minutiae verification algorithm is classifier 1 that yields an average verification accuracy of 88.9% at 0.01% FAR and level-3 pore and ridge verification algorithm is the classifier 2 that yields an average verification accuracy of 91.5% at 0.01% FAR. We evaluate the performance of the fusion algorithms and the results are consistent with multiclassifier face verification. The proposed fusion

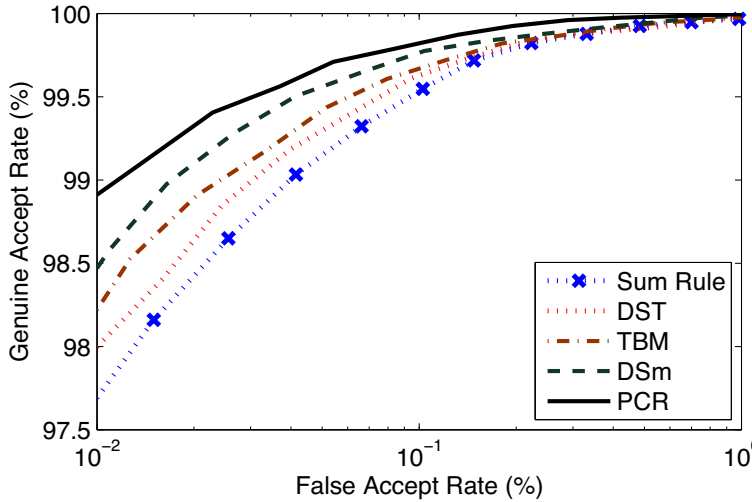

Figure 17.2: ROC of the proposed fusion framework with Sum rule, DS theory fusion, TBM, DSm and PCR rule for *multiclassifier face verification*.

framework with PCR5 rule efficiently handles highly conflicting cases that are caused due to variations in fingerprint image quality compared to other belief model based fusion rules. The proposed framework with PCR5 rule is the most stable fusion algorithm and yields 99.1% average verification accuracy.

17.6 Unification of fusion rules

Existing fusion algorithms, including the proposed fusion framework, may not fulfill all the requirements (i.e. high verification accuracy and low computational time) of a real world biometric system and provide optimal performance for all scenarios. In our recent research paper, we proposed an unification framework to efficiently address both accuracy and time complexity of multimodal biometric fusion [30]. Inspired from Smarandache's theoretical concept [22] and research by Woods *et al.* on dynamic classifier selection [32], the unification algorithm includes a collection of fusion algorithms. For a probe case, the input biometric evidences such as match scores, image quality scores and verification accuracy prior are used to dynamically select the optimal fusion algorithm for information fusion. In [30], we proposed a framework that unifies the sum rule fusion with the DSm fusion rule. The sum rule is simple and effective for cases with minor conflict whereas DSm fusion performs redistribution of conflicting beliefs and yields good performance with highly conflicting information at the

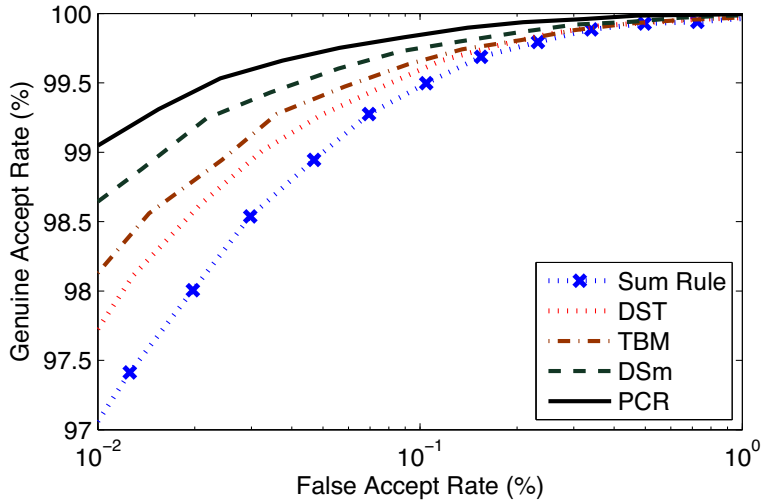

Figure 17.3: ROC of the proposed fusion framework with Sum rule, DS theory fusion, TBM, DSm and PCR rule for *multiclassifier fingerprint verification*.

expense of computational time. The proposed unification framework, in which sum rule and DSm fusion algorithms are unified, improves the verification performance both in terms of accuracy and computational time. More details of the unification algorithm can be obtained from [30].

17.7 Conclusion

This chapter presents a framework for multi-biometric match score fusion when non-ideal conditions cause conflict in the results of different classifiers. The proposed framework uses a belief model based fusion algorithm to effectively fuse the match scores. The framework combines statistical model with belief function models by using density estimation technique, belief model fusion rules and statistical classification. Thus, it has the properties of both statistical fusion approaches as well as belief function rules. Experimental results on multiclassifier face verification and multiclassifier fingerprint verification show that the proposed fusion framework with PCR5 rule yields the best verification accuracy even when the individual biometric classifiers provide highly conflicting match scores. As a future work, the fusion framework can be generalized without Gaussian assumption and the recently proposed DSmP can be included for improved performance.

17.8 Acknowledgments

Portions of the research in this paper use the Notre Dame face database. The authors would like to acknowledge Dr. Smarandache and Dr. Dezert for their valuable suggestions. This research is supported in part through a grant (Award No. 2003-RC-CX-K001) from the Office of Science and Technology, National Institute of Justice, Office of Justice Programs, United States Department of Justice.

17.9 References

[1] `http://www.nd.edu/~cvrl/UNDBiometricsDatabase.html`

[2] J.F. Aguilar, J.O. Garcia, J.G. Rodriguez, and J. Bigun, *Discriminative multimodal biometric authentication based on quality measures*, Pattern Recognition, Vol. 38(5), pp. 777–779, 2005.

[3] T. Ahonen, A. Hadid, and M. Pietikinen, *Face description with local binary patterns: application to face recognition*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 28(12), pp. 2037–2041, 2006.

[4] M. Arif, T. Brouard, and N. Vincent, *A fusion methodology based on Dempster-Shafer evidence theory for two biometric applications*, in Proceedings of 18th International Conference on Pattern Recognition, Vol. 4, pp. 590–593, 2006.

[5] J. Dezert, *Foundations for a new theory of a plausible and paradoxical reasoning*, Information and Security, Vol. 9, pp. 13–57, 2002.

[6] J. Dezert, and F. Smarandache, *Introduction to the fusion of quantitative and qualitative beliefs*, Information and Security, Vol. 20, pp. 9–49, 2006.

[7] D. Dubois and H. Prade, *On the unicity of Dempster rule of combination*, International Journal of Intelligent Systems, Vol. 1, pp. 133–142, 1986.

[8] R.O. Duda, P.E. Hart, and D.G. Stork, *Pattern classification*, Wiley Interscience 2nd edition, ISBN 0-471-05669-3, 2001.

[9] P.J. Flynn, K.W. Bowyer, and P.J. Phillips, *Assessment of time dependency in face recognition: an initial study*, in Proceedings of Audio and Video-Based Biometric Person Authentication, pp. 44–51, 2003.

[10] A.K. Jain, L. Hong, and R. Bolle, *On-line fingerprint verification*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19(4), pp. 302–314, 1997.

[11] X.D. Jiang, W.Y. Yau, and W. Ser, *Detecting the fingerprint minutiae by adaptive tracing the gray level ridge*, Pattern Recognition, Vol. 34(5), pp. 999–1013, 2001.

[12] J. Kittler, M. Hatef, R.P. Duin, and J.G. Matas, *On combining classifiers*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20(3), pp. 226–239, 1998.

[13] E.L. Lehmann and J.P. Romano, *Testing statistical hypotheses*, Springer, 2005.

[14] K. Nandakumar, Y. Chen, S.C. Dass and A.K. Jain, *Likelihood ratio based biometric score fusion*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 30(2), pp. 342–347, 2008.

[15] A. Ross, K. Nandakumar, and A.K. Jain, *Handbook of multibiometrics*, Springer, 1st edition, ISBN: 0-3872-2296-0, 2006.

[16] G. Shafer, *A mathematical theory of evidence*, Princeton University Press, 1976.

[17] S.K. Singh, D.S. Chauhan, M. Vatsa, and R. Singh, *A robust skin color based face detection algorithm*, Tamkang Journal of Science and Engineering, Vol. 6(4), pp. 227–234, 2003.

[18] R. Singh, M. Vatsa, A. Noore, and S.K. Singh, *DS theory classifier fusion with update rule to minimize training time*, IEICE Electronics Express, Vol. 3(20), pp. 429–435, 2006.

[19] R. Singh, M. Vatsa, A. Noore, and S.K. Singh, *Dempster Shafer theory based classifier fusion for improved fingerprint verification performance*, in Proceedings of Indian Conference on Computer Vision, Graphics and Image Processing, LNCS 4338, pp. 941–949, 2006.

[20] R. Singh, M. Vatsa, and A. Noore, *Face recognition with disguise and single gallery images*, Image and Vision Computing, Vol. 37(3), pp. 245–257, 2009.

[21] R. Singh, M. Vatsa, and A. Noore, *Integrated multilevel image fusion and match score fusion of visible and infrared face images for robust face recognition*, Pattern Recognition, Vol. 43(3), pp. 880–893, 2008.

[22] F. Smarandache, *An in-depth look at quantitative information fusion rules*, in Advances and Applications of DSmT for Information Fusion, American Research Press, Chapter 8, pp. 205–236, 2006.

[23] P. Smets and R. Kennes, *The transferable belief model*, Artificial Intelligence, Vol. 66(2), pp. 191–234, 1994.

[24] P. Smets, *Decision making in a context where uncertainty is represented by belief functions*, Physica-Verlag, pp. 17–61, 2002.

[25] P. Smets, *Analyzing the combination of conflicting belief functions*, Information Fusion, Vol.8(4), pp. 387–412, 2007.

[26] Y. Sugie and T. Kobayashi, *Media-integrated biometric person recognition based on the Dempster-Shafer theory*, in Proceedings of 16th International Conference on Pattern Recognition, Vol. 4, pp. 40381–40384, 2002.

[27] B. Ulery, A.R. Hicklin, C. Watson, W. Fellner, and P. Hallinan, *Studies of biometric fusion*, NIST Technical Report IR 7346, 2006.

[28] M. Vatsa, R. Singh, A. Noore, and M. Houck, *Quality-augmented fusion of level-2 and level-3 fingerprint information using DSm theory*, International Journal of Approximate Reasoning, (In press), 2009.

[29] M. Vatsa, R. Singh, A. Noore and S.K. Singh, *Quality induced fingerprint identification using extended feature set*, in Proceedings of IEEE Conference on Biometrics: Theory, Applications and Systems, pp. 1–6, 2008.

[30] M. Vatsa, R. Singh, and A. Noore, *Unification of evidence theoretic fusion algorithms: A case study in level-2 and level-3 fingerprint features*, In IEEE Transactions on Systems, Man, and Cybernetics-A, Vol. 39(1), pp. 47–56, 2009.

[31] F. Voorbraak, *On the justification of Dempsters rule of combination*, Artificial Intelligence, Vol. 48(2), pp. 171–197, 1991.

[32] K. Woods, W.P. Kegelmeyer, and K.W. Bowyer, *Combination of multiple classifiers using local accuracy estimates*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19(4), pp. 405–410, 1997.

[33] R.R. Yager, J. Kacprzyk, and M. Fedrizzi, *Advances in the Dempster-Shafer theory of evidence*, Wiley, 1994.

[34] L. Zadeh, *On the validity of Dempster's rule of combination*, University of California, Berkeley, Memo M 79/24, 1979.

[35] Z. Zivkovic and F. van der Heijden, *Recursive unsupervised learning of finite mixture models*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 26(5), pp. 651–656, 2004.