Unification of Evidence Theoretic Fusion Algorithms: A Case Study in Level-2 and Level-3 Fingerprint Features

Mayank Vatsa, Richa Singh, and Afzel Noore

***Abstract*— This paper formulates an evidence-theoretic multimodal unification approach using belief functions that takes into account the variability in biometric image characteristics. While processing non-ideal images the variation in the quality of features at different levels of abstraction may cause individual classifiers to generate conflicting genuine-impostor decisions. Existing fusion approaches are non-adaptive and do not always guarantee optimum performance improvements. We propose a contextual unification framework to dynamically select the most appropriate evidence-theoretic fusion algorithm for a given scenario. In the first approach, the unification framework uses deterministic rules to select the most appropriate fusion algorithm; while in the second approach, the framework intelligently learns from the input evidences using a 2ν-granular support vector machine. The effectiveness of our unification approach is experimentally validated by fusing match scores from level-2 and level-3 fingerprint features. Compared to existing fusion algorithms, the proposed unification approach is computationally efficient, and the verification accuracy is not compromised even when conflicting decisions are encountered.**

***Index Terms*— Biometric Fusion, Unification, Evidence-theoretic Fusion, Fingerprint Verification**

I. INTRODUCTION

The main advantage of using biometric systems for security applications is their ability to authenticate the true identity of an individual. However, in real world applications, the performance of unimodal biometric systems may suffer due to issues such as non-universality, non-permanence, intraclass variations, poor image quality, noisy data, and matcher limitations [1], [2]. Thus, verification based on unimodal biometric system is not always reliable and researchers have shown that fusion of multiple biometric modalities generally provides higher verification performance [2]-[5]. In literature, there are different forms of biometric information fusion [2], [4], [5]: single biometric - multiple representation, single biometric - multiple matchers, multiple biometrics - multiple representations, and multiple biometrics - multiple matchers. Further, biometric information fusion can be performed at different levels such as data fusion, feature fusion, match score fusion, and decision fusion [2], [4].

Existing biometric fusion algorithms such as sum rule [4] and support vector machine (SVM) fusion [5] yield good performance for some applications or under certain conditions but not universally for all scenarios. Furthermore, the performance of existing match score fusion algorithms decreases when biometric classifiers yield highly conflicting results. For example, if one biometric classifier generates a match score which corresponds to *perfect accept* and another classifier provides a match score which corresponds to *perfect reject* for the same individual, existing fusion algorithms are not able to efficiently perform fusion and matching. The sum rule is very efficient in terms of time complexity but does not provide good performance when dealing with highly conflicting cases. The authors recently proposed match score fusion algorithms [6], [7] using the Dezert Smarandache (DSm) theory of plausible and paradoxical reasoning [8], [9] to efficiently fuse conflicting results. The results show that DSm fusion provides better performance at the expense of higher time complexity. Thus existing fusion algorithms cannot fulfill all the requirements of a real world biometric system and cannot provide optimal performance for all scenarios. To address this issue, Veeramachaneni *et al.* [10] proposed an adaptive multimodal decision fusion algorithm using particle swarm optimization to adaptively combine the decision fusion rules and improve the recognition accuracy. Some commercial products also use ad-hoc techniques to select AND and OR rules depending on the desired security level. However, the complexity of optimizing the algorithm, limitation of fusion algorithms, and incorporating priors are research challenges that still need to be addressed.

In this paper, we propose an unification framework to efficiently address both accuracy and time complexity of multimodal biometric fusion. Our hypothesis is that unification or reconciliation of multiple fusion algorithms should satisfy most of the application requirements and yield better recognition performance. Inspired from Smarandache's theoretical concept [11] and Woods *et al.* research on dynamic classifier selection [12], the unification framework includes a collection of fusion algorithms. As shown in Fig. 1, the unification framework uses the evidences obtained from the input biometric probe data to dynamically select the optimal fusion algorithm. The selected fusion algorithm is then used to compute the fused biometric information. The evidences which serve as input to the unification framework comprise of pertinent and discriminatory attributes such as image quality, features, match scores, and verification prior (precision of true verification score computed from the matcher). Specifically in this paper, we introduce two novel unification frameworks to combine two match score fusion algorithms: (1) Rule-based unification, (2) Learning-based unification. The first unification framework uses a fixed rule-based strategy to unify fusion algorithms. We further extend the fixed rule-based unification strategy by incorporating an intelligent learning technique for adaptive

A shorter version of the manuscript received the Honeywell best student paper award in the First IEEE Conference on Biometrics: Theory, Applications and Systems (BTAS) 2007.

This work was supported in part through a grant (Award No. 2003-RCCX-K001) from the Office of Science and Technology, National Institute of Justice, Office of Justice Programs, United States Department of Justice.

M. Vatsa, R. Singh, and A. Noore are with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV, USA {mayankv, richas, noore}@csee.wvu.edu.

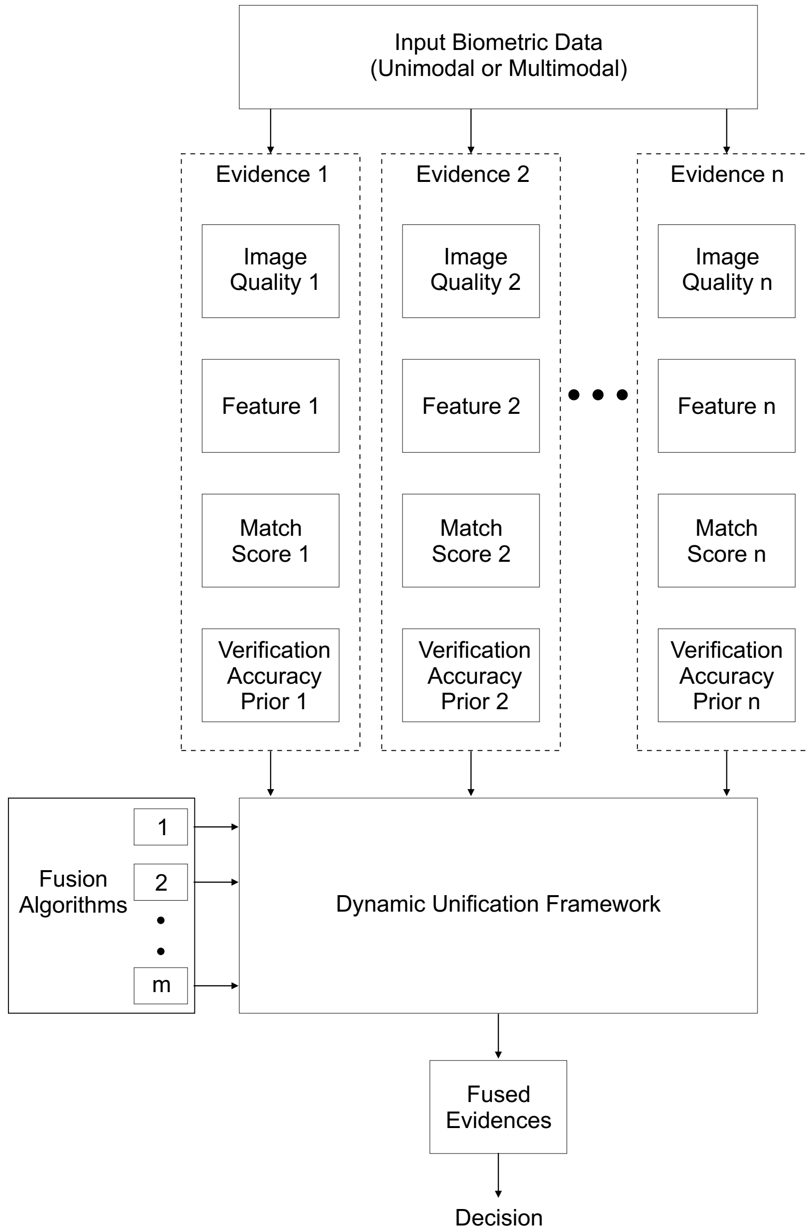
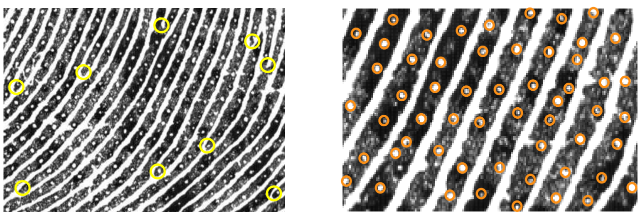


Fig. 1. General concept of the proposed unification framework.

unification.

Existing match score fusion algorithms can be classified into three categories: statistical fusion algorithms [4], learning-based fusion algorithms [13], and evidence theory based fusion algorithms [14]. Previous studies have established that augmenting evidences obtained from representative training data with the input probe data enhances the performance of fusion algorithms [6], [15], [16]. In the proposed unification frameworks, we therefore use evidence-theoretic fusion algorithms with the evidences being image quality, verification prior, and match scores. The first match score fusion algorithm in the proposed unification framework is the evidence-theoretic sum rule which is based on basic probability assignments computed from the match scores. Compared to the traditional sum rule [2], the proposed evidence-theoretic sum rule incorporates prior evidences in terms of image quality and verification accuracy computed using the training dataset. The second fusion algorithm included in the framework is the evidence-theoretic DSm fusion algorithm [7]. This fusion algorithm is based on the theory of plausible and paradoxical reasoning and can optimally fuse the match scores even with highly conflicting results. The two match score fusion algorithms are unified to improve the verification performance.

To demonstrate the effectiveness of the proposed algorithms, we use fingerprint biometrics (single biometrics - multiple matchers) as the case study. Fingerprint images are chosen for this research because the level-2 minutia features and level-3 pore features [17] obtained from fingerprint provide distinguishing information [18], [19]. These features are also used by forensic researchers to establish or verify the identity of an individual. Fig. 2 shows an example of minutia and pore features. Presently, there is limited research undertaken in fusing level-2 and level-3 fingerprint information [6], [18], [19]. Jain *et al.* [18] showed that fusing level-2 and level-3 match scores using min-max normalization and sum rule fusion improves the verification performance. Jain *et al.* [19] further proposed a hierarchical matching scheme which outperforms the sum rule fusion algorithm. Vatsa *et al.* [6] proposed DSm fusion algorithm which efficiently models the conflicting region of level-2 and level-3 match scores and yields a high verification accuracy. A disadvantage of this algorithm is that the computational time is high compared to sum rule fusion. The proposed unification framework adaptively selects an appropriate fusion algorithm to maximize the recognition performance without significantly increasing the computational time. The results also indicate that the proposed evidence-theoretic fusion algorithms and the unification framework perform better than existing match score fusion algorithms.



(a) (b)

Fig. 2. Fingerprint images with (a) minutia features, (b) pore features.

We first present the evidence-theoretic formulation of sum rule and DSm fusion in Section II. In Section III, we extend these fusion algorithms for biometric match score fusion. The proposed unification frameworks are described in Section IV. The characteristics of the fingerprint database and algorithms used for validation are described in Section V. The experimental and statistical results are summarized in Section VI.

II. EVIDENCE-THEORETIC FORMULATION OF SUM RULE AND DSM FUSION

In this section, we describe the formulation of the evidence-theoretic sum rule and DSm theory using belief function models. Since biometric verification is a two-class problem with the classes being *genuine* and *impostor*, both the fusion algorithms are formulated as a two-class problem. These formulations can be extended to any number of classes. Belief functions are defined on the frame of discernment that consists of a finite set of exhaustive and mutually exclusive hypothesis. Let $\Theta = \{\theta_{gen}, \theta_{imp}\}$ be the frame of discernment and θ_{gen} and θ_{imp} be the hypothesis belonging to *genuine* and *impostor* classes respectively.

A. Formulation of Evidence-Theoretic Sum Rule Fusion

In the evidence-theoretic sum rule, the belief function which is also known as the basic probability assignment (*bpa*) is defined as $\overline{m}(\cdot) : \Theta \rightarrow [0, 1]$, such that $\overline{m}(\theta_{gen}) + \overline{m}(\theta_{imp}) = 1$. Here, $\overline{m}(\theta_{gen})$ represents the belief of data being *genuine* and $\overline{m}(\theta_{imp})$ represents the belief of data being *impostor*. For a given match score, if $\overline{m}(\theta_{gen}) = 0.7$ then $\overline{m}(\theta_{imp}) = 0.3$.

To fuse match scores obtained from two different classifiers, the match scores are first transformed into basic probability assignments, $\overline{m}_1(\cdot)$ and $\overline{m}_2(\cdot)$, and then fused using Equations (1) and (2).

$$\overline{m}_{fused}(\theta_{gen}) = \frac{\overline{m}_1(\theta_{gen}) + \overline{m}_2(\theta_{gen})}{2} \tag{1}$$

$$\overline{m}_{fused}(\theta_{imp}) = \frac{\overline{m}_1(\theta_{imp}) + \overline{m}_2(\theta_{imp})}{2} \tag{2}$$

A decision to *accept* or *reject* is made using the pignistic probability ($BetP$) and likelihood ratio test.

$$BetP(\theta_i) = \sum_{\theta_i \in A \subseteq \Theta} \frac{m_{fused}(A)}{|A|} \tag{3}$$

where $i = \{gen, imp\}$. Pignistic probability transforms belief assignment into probability assignments and likelihood ratio test is used with the threshold t for decision making as shown in Equation 4.

$$Decision = \begin{cases} genuine & if \quad \frac{BetP(\theta_{gen})}{BetP(\theta_{imp})} \geq t \\ impostor & otherwise \end{cases} \tag{4}$$

B. Formulation of Evidence-Theoretic DSm Fusion

In contrast to set theory and basic probability assignment, DSm theory [8], [9] uses belief function, also known as generalized basic belief assignment (*gbba*), and operates on the hyperpower set, $D^{\Theta} = \{\emptyset, \theta_{gen}, \theta_{imp}, \theta_{gen} \cup \theta_{imp}, \theta_{gen} \cap \theta_{imp}\}$. Generalized basic belief assignment is defined as $m(\cdot) : D^{\Theta} \rightarrow [0, 1]$ so that the conditions described in Equation 5 are satisfied.

$$\begin{aligned} & m(\emptyset) = 0 \\ & m(\theta_{gen}) + m(\theta_{imp}) + m(\theta_{gen} \cup \theta_{imp}) + \\ & m(\theta_{gen} \cap \theta_{imp}) = 1 \end{aligned} \tag{5}$$

Similar to evidence-theoretic sum rule, $m(\theta_{gen})$ and $m(\theta_{imp})$ are the genuine and impostor beliefs respectively. Further, $m(\theta_{gen} \cap \theta_{imp})$ represents the belief for conflicting region and $m(\theta_{gen} \cup \theta_{imp})$ is the belief that the data belongs to the genuine-impostor feature space. In general, a match is performed with the enrolled identities and the input data belongs to the genuine-impostor feature space. Therefore the value of $m(\theta_{gen} \cup \theta_{imp})$ is set to 0.01. For a given match score, if $m(\theta_{gen}) = 0.6$ and $m(\theta_{imp}) = 0.3$, then from Equation 5, $m(\theta_{gen} \cap \theta_{imp}) = 0.09$. DSm rule of combination for fusing match scores from two classifiers is shown in Equation 6 [8], [9].

$$m_{fused}(A) = \psi(A) \left[S_1(A) + S_2(A) + S_3(A) \right] \tag{6}$$

where, $\psi(A)$ 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,

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

where I_t is the total ignorance and 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 [8], $S_2(A)$ 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. A detailed description of DSm theory along with illustrative examples is presented in [9].

After fusing the match scores using DSm theory, a decision of *accept* or *reject* is made using the pignistic probability and likelihood ratio test.

III. BIOMETRIC MATCH SCORE FUSION

The evidence-theoretic fusion rules described in Section II cannot be directly applied to biometric match score fusion. Match scores obtained from different classifiers are first converted into belief functions using density estimation technique and then the fusion rules are applied on the belief functions. In this section, we describe the algorithm for transforming the match scores into belief functions.

A. Match Score Fusion using Evidence-Theoretic Sum Rule

Let s_1 and s_2 be the two match scores to be fused. We found that the distribution of match scores for every element of $\Theta = \{\theta_{gen}, \theta_{imp}\}$ follows a Gaussian distribution as shown in Equation 7.

$$p(s_i, \overline{\mu}_{ij}, \overline{\sigma}_{ij}) = \frac{1}{\overline{\sigma}_{ij}\sqrt{2\pi}} exp\left[-\frac{1}{2}\left\{\frac{s_i - \overline{\mu}_{ij}}{\overline{\sigma}_{ij}}\right\}^2\right] \quad (7)$$

where $\overline{\mu}_{ij}$ and $\overline{\sigma}_{ij}$ are the mean and standard deviation of the i^{th} classifier corresponding to the j^{th} element of Θ. Therefore the Gaussian distribution is used to compute the basic probability assignment $\overline{m}_i(j)$,

$$\overline{m}_i(j) = \frac{p(s_i, \overline{\mu}_{ij}, \overline{\sigma}_{ij})\overline{\beta}_{ij}}{\sum_{j=1}^{\Theta} p(s_i, \overline{\mu}_{ij}, \overline{\sigma}_{ij})\overline{\beta}_{ij}} \quad (8)$$

where $\overline{\beta}_{ij}$ is the weight factor of classifier i corresponding to the j^{th} element of Θ. $\overline{\beta}_{ij}$ is defined as,

$$\overline{\beta}_{ij} = Q\overline{V}_{ij} \quad (9)$$

Here, Q is the quality score of the input probe image and $\overline{V}_{ij}$ is the verification accuracy prior computed on the training database. Verification accuracy prior is used to attune the classifier's reliability of a probe match by means of errors made on the representative training dataset. Quality score is computed using the redundant discrete wavelet transform based quality assessment algorithm described in [6]. Values of both Q and $\overline{V}_{ij}$ lie in the range of [0, 1]. Basic probabilistic assignments, $\overline{m}_i(j)$, are fused using Equations 1 and 2, and a decision of *accept* or *reject* is made by transforming the fused bpa into probability measure ($BetP$) and then performing the likelihood ratio test.

B. Match Score Fusion using Evidence-Theoretic DSm Theory

Similar to evidence-theoretic sum rule, generalized basic belief assignments of evidence-theoretic DSm fusion, $m_i(j)$, are computed using the Gaussian distribution over $D^\Theta \setminus \{\emptyset, \theta_{gen} \cup \theta_{imp}\} = \{\theta_{gen}, \theta_{imp}, \theta_{gen} \cap \theta_{imp}\}$.

$$m_i(j) = \frac{p(s_i, \mu_{ij}, \sigma_{ij})\beta_{ij}}{\sum_{j=1}^{|D^\Theta|-2} p(s_i, \mu_{ij}, \sigma_{ij})\beta_{ij}} \quad (10)$$

where μ_{ij}, σ_{ij}, and β_{ij} are the mean, standard deviation, and weight factor of the i^{th} classifier corresponding to the j^{th} element of $D^\Theta \setminus \{\emptyset, \theta_{gen} \cup \theta_{imp}\}$. β_{ij} is defined as,

$$\beta_{ij} = QV_{ij} \quad (11)$$

Here, V_{ij} is the verification accuracy prior computed on the training database and Q is the quality score [6] of the probe image. Finally, generalized basic belief assignments, $m_i(j)$, are fused using the DSm rule of combination (Equation 6) and a decision of *accept* or *reject* is determined using the fused *gbba*, pignistic probability, and likelihood ratio test.

IV. FRAMEWORK FOR UNIFICATION OF FUSION ALGORITHMS

Evidence theoretic sum rule is simple and effective for cases with minor conflict. On the other hand, evidence theoretic DSm fusion performs redistribution of conflicting beliefs and yields good performance with highly conflicting information at the expense of computational time. Our hypothesis is that the unification of these two algorithms should provide better verification performance both in terms of accuracy and time. This section describes the two proposed unification frameworks in which evidence-theoretic sum rule and DSm fusion algorithms are unified to improve the verification performance. The rule-based unification is explained first followed by the adaptive unification using Support Vector Machine learning.

A. Rule-based Unification

Fig. 3 shows the steps involved in the proposed rule-based unification framework. In the rule-based unification, the fixed linear rule shown in Equations 12 and 13 is used to dynamically select the fusion algorithm. The procedure for unification is described as follows:

1) $\overline{m}_i(j)$ is computed over $\Theta = \{\theta_{gen}, \theta_{imp}\}$ where $i = 1, 2$ and $j \in \Theta$. The evidence-theoretic sum rule is used if the conditions in Equations 12 or 13 are satisfied.

$$\begin{aligned} \overline{m}_1(\theta_{gen}) &> \overline{m}_1(\theta_{imp}) + \epsilon_1 \\ \overline{m}_2(\theta_{gen}) &> \overline{m}_2(\theta_{imp}) + \epsilon_2 \end{aligned} \quad (12)$$

$$\begin{aligned} \overline{m}_1(\theta_{gen}) + \epsilon_1 &< \overline{m}_1(\theta_{imp}) \\ \overline{m}_2(\theta_{gen}) + \epsilon_2 &< \overline{m}_2(\theta_{imp}) \end{aligned} \quad (13)$$

where, ϵ_1 and ϵ_2 are the error parameters of the two classifiers.

2) If both the above conditions are not satisfied, i.e., when the matchers provide highly conflicting results, then

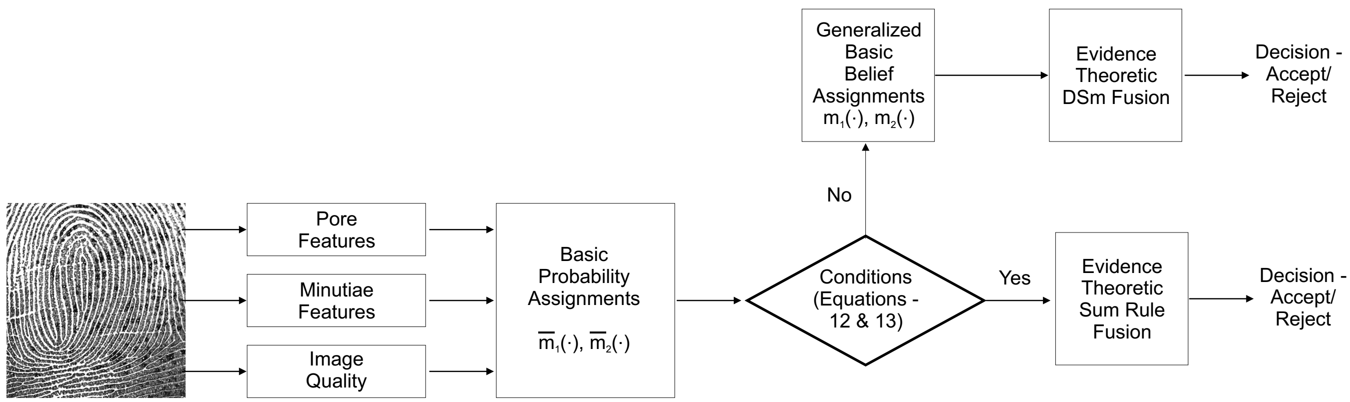


Fig. 3. Proposed rule-based unification framework.

the DSm fusion algorithm is applied. In such cases, $m_i(j)$ is computed over $D^\Theta \setminus \{\emptyset, \theta_{gen} \cup \theta_{imp}\} = \{\theta_{gen}, \theta_{imp}, \theta_{gen} \cap \theta_{imp}\}$ and fusion is performed using Equation 6.

B. Adaptive Unification using 2ν-GSVM Learning

Unification using the rule-based approach has certain limitations. In the rule-based approach, we first compute basic probability assignment and then the unification conditions (Equations 12 and 13) are evaluated to decide whether the evidence-theoretic sum rule or DSm fusion algorithm should be selected. If the unification condition suggests the use of evidence-theoretic DSm fusion, both basic probability assignments (*bpa*) and generalized basic belief assignments (*gbba*) are computed which require additional time. Further, the fixed rule-based unification approach becomes complex if additional fusion rules have to be incorporated in the unification framework and requires some form of optimization. To minimize such complexities, we propose an adaptive unification framework that intelligently learns from the input evidences and selects the appropriate fusion algorithm.

In the proposed adaptive unification framework, we can use any learning strategy to select an appropriate fusion algorithm. Support Vector Machine (SVM) has been widely used in literature for efficient data classification [20]. Chew *et al.* [21] proposed 2ν-SVM as a variant of SVM to address the challenges of SVM such as reduction in time complexity and classification with disparate number of training samples per class. In our previous research [5], we found that for multimodal fusion, 2ν-SVM provides better classification with lower time complexity compared to the classical SVM [20]. Further, Tang *et al.* [22] proposed another variant of SVM by applying granular computing to improve the data classification and time complexity. Granular computing is a knowledge-oriented divide and conquer approach to problem solving in which information is divided into subproblems and these subproblems are solved individually at different granularity levels [23]-[26]. We used these concepts to incorporate granular computing in 2ν-SVM and formulate the 2ν-Granular SVM [7]. 2ν-GSVM embodies the properties of both granular computing and 2ν-SVM, and uses multiple SVMs to learn both local and global properties of the input data at different granularity levels. In [7], it has also been shown that 2ν-GSVM is more adaptive to the data distribution and has lower complexity compared to the classical SVM and 2ν-SVM. Detailed formulation of 2ν-GSVM is presented in [7]. In the proposed adaptive unification framework, we thus use 2ν-GSVM to intelligently learn from the input evidences and select the most appropriate fusion algorithm for optimal performance. Fig. 4 illustrates the computational steps involved in the adaptive unification framework. Image quality and match scores obtained from minutiae and pores matching are used as input to the 2ν-GSVM classifier. Depending on the output of the 2ν-GSVM classifier, either the evidence-theoretic DSm fusion or evidence-theoretic sum rule is selected for fusion. The adaptive unification is divided into two stages: (1) training and (2) classification.

Training 2ν-GSVM: We train the 2ν-GSVM for unification of the fusion algorithms using a labeled training database. The training algorithm is described as follows:

1) Let the input training data be $\{\mathbf{x_i}, y_i\}$ where $i = 1, ..., N$. N is the total number of training data, $\mathbf{x_i}$ is the i^{th} data vector that belongs to the binary class y_i. $\mathbf{x_i}$ contains the image quality score and two match scores obtained from the minutiae and pores matching. $y_i \in (+1, -1)$ is the label such that +1 belongs to the data that should be fused using DSm fusion and -1 belongs to the data that should be fused using the evidence-theoretic sum rule.
2) 2ν-GSVM is trained using radial basis function kernel such that when the output of 2ν-GSVM ≥ 0, the evidence-theoretic DSm fusion is performed and when the output of 2ν-GSVM < 0, evidence-theoretic sum rule fusion is performed.

Classification and Unification: At the probe level, the trained 2ν-GSVM is used to perform classification and unification. The classification algorithm dynamically selects the most appropriate fusion algorithm depending on the quality score and input probe match scores. The steps involved in the classification and unification are described as follows:

1) The image quality score along with the match scores obtained from minutiae and pore matching are provided

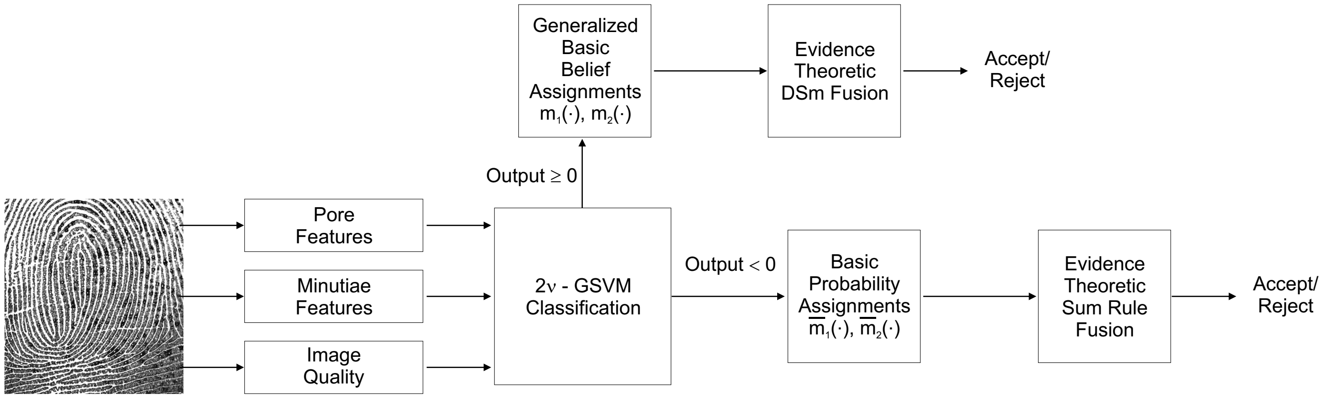


Fig. 4. Proposed adaptive unification framework using 2ν-GSVM.

as input to the classification algorithm.

2) Trained 2ν-GSVM classifier is used to classify the input probe data. The classification algorithm selects either the evidence-theoretic DSm fusion or evidence-theoretic sum rule fusion to fuse the probe match scores.
3) Depending on the classification result of the 2ν-GSVM classifier, an appropriate fusion algorithm is applied to compute the fused match score and a decision of *accept* or *reject* is made.

The adaptive unification framework thus dynamically selects the most appropriate fusion algorithm to improve the verification accuracy and decrease the computational time. The framework can be further generalized to include other fusion schemes with more than two classifiers for other multimodal biometric scenarios.

V. DATABASE AND ALGORITHMS USED FOR VALIDATION

The proposed algorithms are validated using level-2 minutiae and level-3 pores based fingerprint recognition algorithm on a 1000 ppi fingerprint database. In this section, we briefly describe the database and the algorithms used for validation.

A. Fingerprint Database

To validate the proposed unification framework, a fingerprint database obtained from law enforcement agency is used. This 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 and level-3 features. From each class, two good quality and one poor quality fingerprints are selected for training the evidence-theoretic sum rule, evidence-theoretic DSm fusion, rule-based unification, and 2ν-GSVM adaptive unification framework. The remaining seven images per class are used as gallery and probe. We thus have 11,550 genuine matches $\left(\frac{550\times7\times6}{2}\right)$ and 7,397,775 impostor matches $\left(\frac{550\times7\times549\times7}{2}\right)$ using the gallery and probe database.

B. Algorithms used for Validation

Fingerprint image quality and match scores corresponding to minutiae and pore features are computed using existing image quality assessment and feature extraction algorithms which are briefly described below.

Redundant Discrete Wavelet Transform based Quality Assessment Algorithm: The RDWT image quality assessment algorithm [6] is used to compute the quality score, Q, of fingerprint images. The algorithm extracts the edge regions, non-edge regions and noisy regions, and assigns appropriate weights to each subband of the RDWT decomposition. This information is combined to generate the composite quality score that provides both frequency and temporal content of the fingerprint at different resolution levels. The original quality assessment algorithm generates the quality score, Q', in the range of [0, 1], where 0.5 represents the highest quality and 0 and 1 represent the lowest quality. We normalize the quality score using Equation 14.

$$Q = \begin{cases} \frac{Q'}{0.5} & if \quad 0 \leq Q' \leq 0.5 \\ \frac{1-Q'}{0.5} & if \quad 0.5 < Q' \leq 1 \end{cases} \tag{14}$$

where Q is the normalized quality score and the value lies in the range of [0, 1]. Quality score of 0 represents the worst quality and 1 represents the best quality image. Fig. 5 shows examples of different quality fingerprint images and their respective quality scores.

Minutia-based Verification Algorithm: To extract minutiae from a fingerprint image, a ridge tracing minutiae extraction algorithm [27] is used. The extracted minutiae are matched using a dynamic bounding box based matching algorithm [28]. This algorithm generates a match score, which is normalized in the range of [0, 1] using score normalization technique [29]. If the value of the normalized match score is 0, it represents perfect *reject* and if the normalized match score is 1, it represents perfect *accept*.

Pore-based Verification Algorithm: To extract the pore features, we use the verification algorithm described by Kryszczuk *et al.* [30], [31]. This algorithm extracts pore information from high resolution fingerprint images by applying different techniques such as correlation based alignment, Gabor filtering, binarization, morphological filtering, and tracing. The match score obtained from this algorithm is a normalized similarity score in the range of [0, 1].

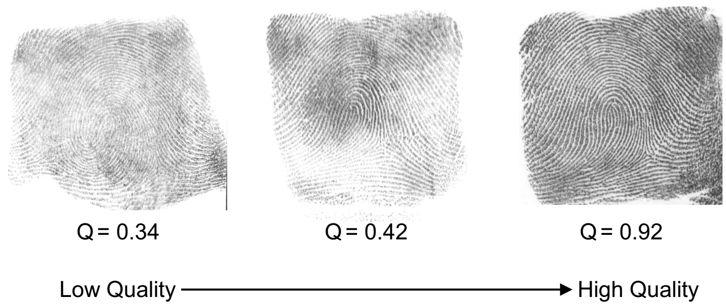


Fig. 5. Quality score of fingerprints obtained using redundant discrete wavelet transform based quality assessment algorithm [6].

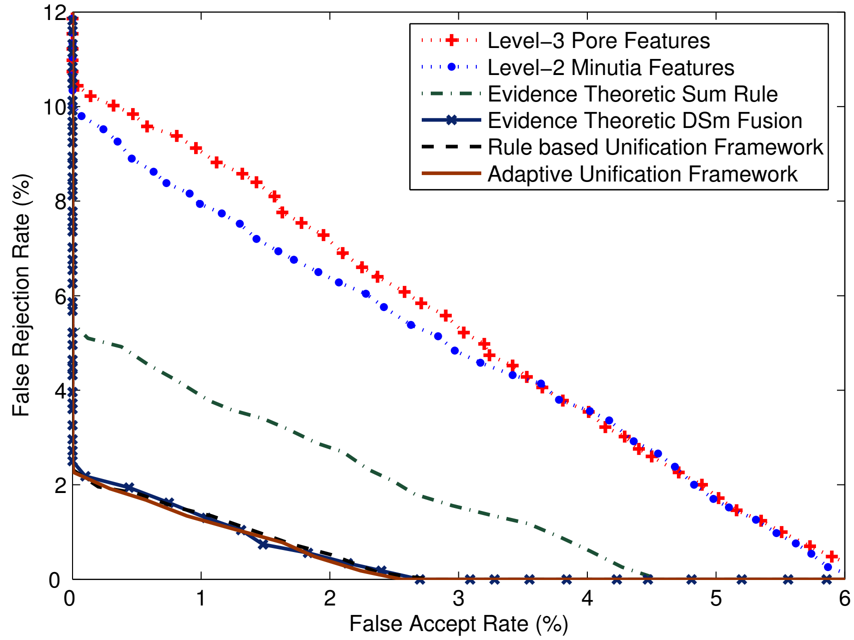
Existing Fusion Algorithms used for Comparison: To compare the performance of the proposed unification framework, we use three existing fusion algorithms namely sum rule [4], SVM fusion [13], and Dempster Shafer (DS) theory based fusion algorithm [14]. Among the existing algorithms, SVM fusion by Aguilar *et al.* [13] incorporates image quality score with the match scores. To evaluate the performance of the SVM fusion algorithm, we have used the same quality scores computed using the RDWT quality assessment algorithm [6].

VI. EXPERIMENTAL RESULTS

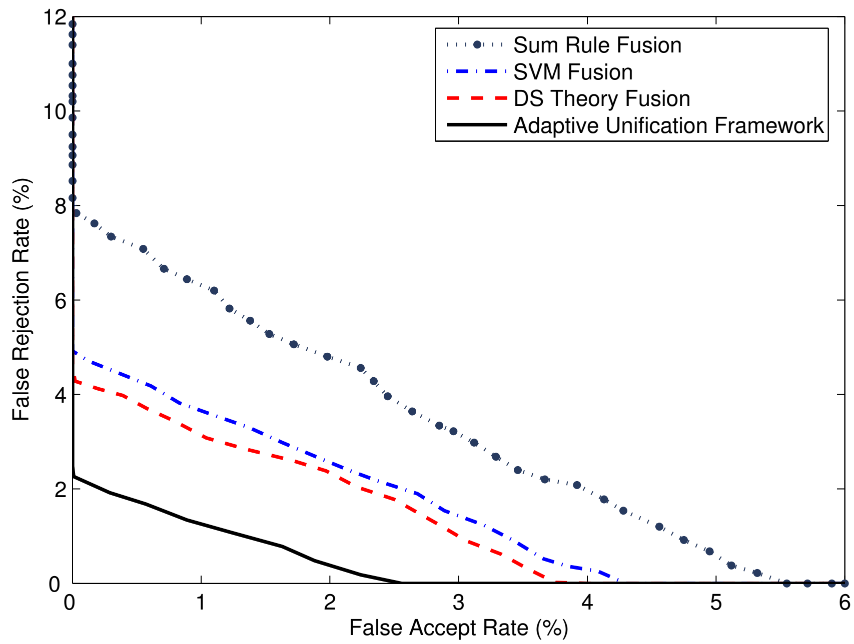
The effectiveness of the proposed unification framework is demonstrated experimentally by computing the verification performance of fingerprint biometrics. We perform two experiments to evaluate the performance of the proposed evidence-theoretic fusion algorithms and the unification framework. The first experiment computes the improvement in verification performance due to level-2 and level-3 match score fusion and the unification framework. The second experiment compares the performance of the proposed evidence-theoretic fusion algorithms and unification framework with existing statistical match score fusion algorithm [2], learning-based match score fusion algorithm [13], and DS theory based fusion algorithm [14]. This experiment also evaluates the performance of the unification framework and existing match score fusion algorithms with low quality and high quality fingerprint images. The proposed algorithms are trained using the training database to compute the mean ($\overline{\mu}_{ij}, \mu_{ij}$), standard deviation ($\overline{\sigma}_{ij}, \sigma_{ij}$), verification accuracy prior ($\overline{V}_{ij}, V_{ij}$), and the error parameters (ϵ_1, ϵ_2) for the evidence-theoretic fusion and unification algorithms. The training database is also used to train the 2ν-GSVM classifier for adaptive unification.

A. Performance Evaluation of Proposed Unification Framework

In this experiment, we compute the verification performance using level-2 minutiae features, level-3 pore features, evidence-theoretic sum rule, evidence-theoretic DSm fusion, and the unification framework at 0.001% False Accept Rate (FAR) (verification accuracy at 0.001% FAR shows genuine accept rate at a very low false accept rate). As shown in Table I and Fig. 6(a), level-3 pore features yield a verification accuracy of 89.49% which is 0.52% less than the verification accuracy of level-2 minutia features. This is because, there are large number of pore features in a fingerprint image which tends to increase the false rejection rate. Moreover, the pore extraction algorithm [30] is not reliable when the image is of lower quality due to deformation and other extraneous noise. When the match scores of level-2 minutia features and level-3 pore features are fused using the proposed evidence-theoretic sum rule, verification accuracy improves by 4.69%. DSm fusion algorithm further improves the verification performance and provides an accuracy of 97.6%. The performance of evidence-theoretic sum rule reduces when the minutia-based classifier and pore-based classifier yield highly conflicting results. In such cases, DSm match score fusion algorithm operates on the conflicting region and provides optimal decision using prior information of the unimodal classifiers. The DSm match score fusion algorithm thus provides better verification performance. Finally, the proposed unification frameworks yield a verification accuracy of 97.63% which is slightly better than the DSm fusion algorithm. We found that there are 334 instances when the DSm fusion yields correct classification and evidence-theoretic sum rule provides incorrect classification. Further, there are three instances when the DSm fusion produces incorrect results and the evidence-theoretic sum rule provides correct results. However, in both the unification frameworks these cases are correctly classified. Another advantage of using the unification frameworks over DSm theory is the computation time. As shown in Table I, the average verification time computed on 3.2 P-IV processor with 1GB RAM under Matlab environment using DSm fusion algorithm (including quality assessment, feature extraction, and matching) is approximately 23 seconds. In contrast, the rule-based unification framework takes approximately 18 seconds and the adaptive unification requires around 16 seconds. This shows that the unification frameworks provide higher verification accuracy without significantly increasing the computational time. On comparing both the unification frameworks, we found that the 2ν-GSVM based adaptive unification yields better performance compared to the rule-based unification. Although for this particular case study, the verification accuracies are same, but the computational complexity of the rule-based unification is higher than the adaptive unification. Further, as mentioned in Section IV-B, extending the adaptive unification framework to more than two fusion algorithms is easier and more logical compared to the rule-based unification.



(a)



(b)

Fig. 6. (a) ROC plot demonstrating the verification performance of the evidence-theoretic fusion algorithms and the proposed unification framework using level-2 and level-3 fingerprint features. (b) ROC plot comparing the verification performance of existing fusion algorithms and the proposed adaptive unification framework.

TABLE I

COMPARING THE VERIFICATION PERFORMANCE OF THE PROPOSED UNIFICATION FRAMEWORK WITH EXISTING MATCH SCORE FUSION ALGORITHMS USING LEVEL-2 AND LEVEL-3 FINGERPRINT FEATURES. VERIFICATION ACCURACY IS COMPUTED AT 0.001% FALSE ACCEPT RATE (FAR).

Algorithms	Complete Database		Low Quality Images		High Quality Images	
	Verification Accuracy (%)	Time (seconds)	Verification Accuracy (%)	Time (seconds)	Verification Accuracy (%)	Time (seconds)
Level-3 Pore Features [30], [31]	89.49	12.08	72.45	12.14	91.14	11.97
Level-2 Minutiae Features [27], [28]	90.01	3.15	84.60	3.19	93.57	3.13
Sum Rule Fusion [4]	92.08	15.29	89.73	15.38	96.10	15.16
Evidence-Theoretic Sum Rule Fusion	94.70	16.03	92.49	16.06	96.95	16.01
SVM Fusion [13]	95.15	18.31	92.37	18.33	97.12	18.30
DS Theory Fusion [14]	95.82	20.24	92.51	20.27	97.33	20.23
Evidence-Theoretic DSm Fusion	97.60	23.47	95.97	23.48	98.81	23.45
Rule-based Unification Framework	97.63	18.39	96.03	22.02	98.81	16.42
Adaptive Unification Framework	97.63	16.48	96.03	18.57	98.81	16.41

B. Comparing Performance of Unification Framework with Existing Match Score Fusion Algorithms

We next show the efficacy of the proposed fusion algorithms and the unification framework by comparing with existing match score fusion algorithms such as sum rule [4], SVM fusion [13], and DS theory fusion algorithm [14]. We first compute the verification performance of all the algorithms on the complete gallery-probe database containing seven fingerprint images. ROC plots in Fig. 6(b) and the second column of Table I demonstrate the results of this experiment. The results show that existing fusion algorithms improve the verification performance by around 2-6% when the match scores from level-2 and level-3 features are combined, while the proposed algorithms improve the accuracy by around 4-8%. The lower performance of existing fusion algorithms is due to the low image quality and matcher limitations. For example, low image quality and noise leads to spurious minutiae in a fingerprint image which reduces the performance of level-2 features. These factors lead to the generation of conflicting match scores from the two fingerprint classifiers. The proposed unification framework efficiently augments quality score and verification accuracy priors along with match scores and thus improves performance.

To further accentuate the importance of the proposed algorithms, we compute the verification accuracy with low quality and high quality fingerprint images separately. In this experiment, we study the reason behind lower performance of existing fusion algorithms and how the unification framework manages to perform well with conflicting cases. We first use the RDWT quality assessment algorithm [6] to divide the gallery-probe database into two parts: low quality fingerprint database and high quality fingerprint database. The low quality database contains fingerprint images with quality score between 0 and 0.7 ($0 \leq Q \leq 0.7$) whereas the high quality database contains images with quality score between 0.7 and 1.0 ($0.7 < Q \leq 1.0$). In the low quality database, there are more than 1600 genuine matches and in the high quality database, there are more than 3300 genuine matches. Both the low quality and high quality databases are used to compute the verification accuracy of level-2 and level-3 fingerprint recognition algorithms, existing and proposed fusion algorithms, and the proposed rule-based and adaptive unification frameworks at 0.001% FAR. The last four columns of Table I show the verification accuracy and the average time required for all these algorithms. Analysis of the results are summarized below:

- Relative performance gain of 33.1% is observed with the evidence-theoretic sum rule compared to the traditional sum rule. Specifically, with low quality fingerprint images, the proposed evidence-theoretic sum rule shows significant improvement compared to the sum rule. This improvement is because the evidence-theoretic sum rule operates on belief functions and takes into account the image quality and verification accuracy prior.
- The evidence-theoretic DSm fusion outperforms all the match score fusion algorithms and shows relative performance gain of 42.6% and 50.5% compared to DS theory fusion and SVM fusion, respectively. With the low quality fingerprint images, level-3 pore features and level-2 minutia features yield greater number of conflicting results and the performance of existing fusion algorithm suffer due to these cases. On the other hand, as mentioned in Section VI-A, DSm fusion yields better performance with conflicting cases by modeling the overlapping/conflicting region, using priors, and quality score to make optimal decision.
- The proposed unification framework yields the best verification performance. With high quality fingerprint images, the verification accuracies of the unification frameworks and evidence-theoretic DSm fusion are identical. However, with low quality images, the unification framework shows minor improvement over DSm fusion. The main advantage of the unification framework over DSm fusion is the reduction in time complexity. For identity verification using the complete database, the adaptive unification framework requires an average of 16.48 seconds which is 7 seconds faster than the evidence-theoretic DSm fusion and only 0.45 seconds slower than the evidence-theoretic sum rule. Also, the adaptive unification framework is faster than the rule-based unification framework due to the use of fast 2ν-GSVM classification which takes less than 0.2 seconds to perform classification.
- The experimental results also suggest that in any scenario, the performance of the unification framework will be at

least equal to the performance of the weakest fusion rule in the framework. Further, the time required by the unification framework will be less than or equal to the time required by the computationally most expensive fusion algorithm.

C. Statistical Evaluation using Half Total Error Rate

Experimental evaluations shown by verification accuracy and ROC curves demonstrate that the unification frameworks perform better than existing fusion algorithms. However, these results do not justify that the proposed algorithms are statistically better than existing algorithms because the performance of a biometric system greatly depends on the database size and the images present in the database [32]. The statistical differences cannot be represented completely by the ROC plots and verification accuracies. To statistically evaluate the verification performance obtained from the proposed fusion, unification, and existing fusion algorithms, we use the Half Total Error Rate (HTER) significance test [16], [33] at 0.001% FAR.

To aid the statistical interpretation, half total error rate is defined by combining false accept rate and false reject rate.

$$HTER = \frac{FAR + FRR}{2} \tag{15}$$

Equal error rate is a special case of HTER when FAR = FRR. Further, confidence intervals are computed around HTER as $HTER \pm \sigma \cdot Z_{\alpha/2}$. σ and $Z_{\alpha/2}$ are computed using Equations 16 and 17 [33].

$$\sigma = \sqrt{\frac{FAR(1-FAR)}{4 \cdot NI} + \frac{FRR(1-FRR)}{4 \cdot NG}} \tag{16}$$

$$Z_{\alpha/2} = \begin{cases} 1.645 & for\ 90\%\ CI \\ 1.960 & for\ 95\%\ CI \\ 2.576 & for\ 99\%\ CI \end{cases} \tag{17}$$

NG is the total number of genuine scores and NI is the total number of impostor scores. In our experiments, $NG = 11,550$ and $NI = 7,397,775$. Table II summarizes the HTER and confidence intervals at 0.001% FAR. The statistical test shows that the proposed unification frameworks provide the lowest HTER and with 95% confidence, the confidence interval lies in between $1.19 \pm 0.14\%$. It also shows that on a database similar to the fingerprint database used in our experiments, with any number of classes, HTER of the unification framework will be the lowest.

TABLE II

HTER PERFORMANCE OF FINGERPRINT VERIFICATION ALGORITHMS, EXISTING FUSION ALGORITHMS, EVIDENCE-THEORETIC FUSION ALGORITHMS, AND THE UNIFICATION FRAMEWORKS. VERIFICATION ACCURACY IS COMPUTED AT 0.001% FALSE ACCEPT RATE (FAR).

Algorithms	HTER	Confidence Interval		
		90%	95%	99%
Level-3 Pore Features [30], [31]	5.25	0.47	0.56	0.74
Level-2 Minutia Features [27], [28]	4.99	0.46	0.55	0.72
Sum Rule Fusion [4]	3.96	0.41	0.49	0.65
Evidence-Theoretic Sum Rule	2.65	0.34	0.41	0.54
SVM Fusion [13]	2.43	0.33	0.39	0.52
DS Theory Fusion [14]	2.09	0.31	0.37	0.48
DSm Fusion	1.20	0.23	0.28	0.37
Rule-based Unification Framework	1.19	0.23	0.28	0.37
Adaptive Unification Framework	1.19	0.23	0.28	0.37

VII. CONCLUSION

The performance of existing biometric fusion algorithms is compromised when individual classifiers provide highly conflicting results due to non-ideal data acquisition and variation in data quality. In this paper, we proposed evidence-theoretic sum rule and DSm fusion algorithms using basic probability assignments and belief functions. This formulation includes image quality and verification accuracy prior for improving the recognition performance. We further proposed two unification frameworks that dynamically select the most appropriate evidence-theoretic fusion algorithm. The first unification framework is a rule-based approach in which either the evidence-theoretic sum rule or evidence-theoretic DSm fusion is applied depending on the given scenario. The second unification framework extends the rule-based unification framework by using intelligent 2ν-GSVM classification to dynamically select the appropriate fusion algorithm for the best performance. Both the unification frameworks are case based approaches and can be used to improve the verification performance. To validate the proposed algorithms, case study on fingerprint biometrics is presented using level-2 minutia and level-3 pore features (single biometrics - multiple matchers). The experimental and statistical results show a major improvement in verification performance by using the evidence-theoretic fusion algorithms and unification framework compared to existing fusion algorithms. Among all the fusion algorithms, the adaptive unification framework yields the best verification accuracy with lower time complexity.

The proposed unification framework can also be used for other multimodal scenarios such as match score fusion of multiple biometric modalities (face and fingerprint, or face and iris). However, more research is required to expand the unification framework to include multi-matchers, multilevel fusion and multibiometrics. We intend to make the algorithm more general and increase the applicability to other multibiometric scenarios, to incorporate mixture model based density estimation in the fusion algorithms.

VIII. ACKNOWLEDGMENTS

The authors would like to thank Dr. S.K. Singh for his support in database collection. The authors also acknowledge Dr. F. Smarandache and Dr. J. Dezert for their valuable suggestions and the reviewers for their helpful and constructive comments.

REFERENCES

[1] A.K. Jain, R. Bolle, and S. Pankanti, *BIOMETRICS: personal identification in networked society*, Kluwer Academic Publishers, 1999.

[2] A. Ross, K. Nandakumar, and A.K. Jain, *Handbook of multibiometrics*, Springer Publishers, 2006.
[3] J. Kittler, M. Hatef, R.P. Duin, and J.G. Matas, "On combining classifiers," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 3, 1998, pp. 226-239.
[4] A. Ross and A.K. Jain, "Information fusion in biometrics," Pattern Recognition Letters, vol. 24, no. 13, 2003, pp. 2115-2125.
[5] R. Singh, M. Vatsa, and A. Noore, "Intelligent biometric information fusion using support vector machine," Soft Computing in Image Processing: Recent Advances by Springer edited by M. Nachtegael, D. Van der Weken, E. E. Kerre, and W. Philips, Chapter 12, 2006, pp. 327-350.
[6] M. Vatsa, R. Singh, A. Noore, and M.M. Houck, "Quality-augmented fusion of level-2 and level-3 fingerprint information using DSm theory," International Journal of Approximate Reasoning, 2008, http://dx.doi.org/10.1016/j.ijar.2008.01.009.
[7] 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 - Special Issue on Multimodal Biometrics, vol. 41, no. 3, 2008, pp. 880-893.
[8] J. Dezert, "Foundations for a new theory of a plausible and paradoxical reasoning," Information and Security Journal, vol. 9, 2002, pp. 13-57.
[9] F. Smarandache and J. Dezert, *Advances and applications of DSmT for information fusion*, American Research Press, 2004.
[10] K. Veeramachaneni, L.A. Osadciw, and P.K. Vasrhney, "An adaptive multimodal biometric management algorithm," IEEE Transactions on Systems Man and Cybernetics, Part C: Applications and Reviews, vol. 35, no. 3, 2005, pp. 344-356.
[11] F. Smarandache, "An in-depth look at quantitative information fusion rules," Advances and Applications of DSmT for Information Fusion, American Research Press, vol. 2, Chapter 8, 2006, pp. 205-236.
[12] 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, no. 4, 1997, pp. 405-410.
[13] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigün, "Discriminative multimodal biometric authentication based on quality measures," Pattern Recognition, vol. 38, no. 5, 2005, pp. 777-779.
[14] R. Singh, M. Vatsa, A. Noore and S.K. Singh, "Dempster shafer theory based classifier fusion for improved fingerprint verification performance," Indian Conference on Computer Vision, Graphics and Image Processing, vol. 4338, 2006, pp. 941-949.
[15] J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia, and A.K. Jain, "Incorporating image quality in multi-algorithm fingerprint verification," Proceedings of International Conference on Biometrics, 2006, pp. 213-220.
[16] E.S. Bigün, J. Bigün, B. Duc, and S. Fischer, "Expert conciliation for multi modal person authentication systems by bayesian statistics," Proceedings of Audio Video based Biometric Person Authentication, 1997, pp. 291-300
[17] CDEFFS: The ANIS/NIST committee to define an extended fingerprint feature set, *http://fingerprint.nist.gov/standard/cdeffs/index.html*, 2007.
[18] A.K. Jain, Y. Chen, and M. Demirkus, "Pores and ridges: fingerprint matching using level 3 features," Proceedings of International Conference on Pattern Recognition, vol. 4, 2006, pp. 477-480.
[19] A.K. Jain, Y. Chen, and M. Demirkus, "Pores and ridges: high resolution fingerprint matching using level 3 features," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 1, 2007, pp. 15-27.
[20] V. Vapnik, S.E. Golowich, and A. Smola, "Support vector method for function approximation, regression estimation and signal processing," Advances in Neural Information Processing Systems, vol. 9, 1997, pp. 281-287.
[21] H.G. Chew, C.C. Lim, and R.E. Bogner, "An implementation of training dual-ν support vector machines," Optimization and Control with Applications edited by L. Qi, K.L. Teo and X. Yang, Kluwer, 2005, pp. 157182.
[22] Y.C. Tang and Y.-Q. Zhang, "Granular support vector machines with data cleaning for fast and accurate biomedical binary classification," Proceedings of International Conference on Granular Computing, 2005, pp. 262-265.
[23] A. Bargiela and W. Pedrycz, *Granular computing: an introduction*, Kluwer International Series in Engineering and Computer Science, 2002.
[24] A. Bargiela and W. Pedrycz, "The roots of granular computing," Proceedings of IEEE International Conference on Granular Computing, 2006, pp. 806-809.
[25] Y.H. Chen and Y.Y. Yao, "Multiview intelligent data analysis based on granular computing," Proceedings of IEEE International Conference on Granular Computing, 2006, pp. 281-286.
[26] Y.Y. Yao, "Perspectives of granular computing," Proceedings of IEEE International Conference on Granular Computing, vol. 1, 2005, pp. 85-90.
[27] X.D. Jiang, W.Y. Yau, and W. Ser, "Detecting the fingerprint minutiae by adaptive tracing the gray level ridge," Pattern Recognition, vol. 34, no. 5, 2001, pp. 999-1013.
[28] A.K. Jain, L. Hong, and R. Bolle, On-line Fingerprint Verification, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 4, 1997, pp. 302-314.
[29] A.K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," Pattern Recognition, vol. 38, no. 12, 2005, pp. 2270-2285.
[30] K. Kryszczuk, A. Drygajlo, and P. Morier, "Extraction of level 2 and level 3 features for fragmentary fingerprints," Proceedings of 2nd COST275 Workshop, 2004, pp. 83-88.
[31] K. Kryszczuk, P. Morier, and A. Drygajlo, "Study of the distinctiveness of level 2 and level 3 features in fragmentary fingerprint comparison," Proceedings of ECCV International Workshop on Biometric Authentication, Lecture Notes in Computer Science, Springer-Verlag, vol. 3087, 2004, pp. 124-133.
[32] R.M. Bolle, N.K. Ratha, and S. Pankanti, "Performance evaluation in 1:1 biometric engines," Proceedings of Sinobiometrics, 2004, pp. 27-46.
[33] S. Bengio and J. Marièthoz, "A statistical significance test for person authentication," Proceedings of Odyssey: The Speaker and Language Recognition Workshop, 2004, pp. 237-244.

Mayank Vatsa is a graduate research assistant in the Lane Department of Computer Science and Electrical Engineering at West Virginia University. He is currently pursuing his Doctoral degree in Computer Science. He had been actively involved in the development of a multimodal biometric system which includes face, fingerprint, signature, and iris recognition at Indian Institute of Technology Kanpur, India from July 2002 to July 2004. His current areas of interest are pattern recognition, image processing, uncertainty principles, biometric authentication, watermarking, and information fusion. Mayank has more than 65 publications in refereed journals, book chapters, and conferences. He has received four best paper awards. He is a member of the IEEE, Computer Society, and ACM. He is also a member of Phi Kappa Phi, Tau Beta Pi, Sigma Xi, Upsilon Pi Epsilon, and Eta Kappa Nu honor societies.

Richa Singh is a graduate research assistant in the Lane Department of Computer Science and Electrical Engineering at West Virginia University. She is currently pursuing her Doctoral degree in Computer Science. She had been actively involved in the development of a multimodal biometric system which includes face, fingerprint, signature, and iris recognition at Indian Institute of Technology Kanpur, India from July 2002 to July 2004. Her current areas of interest are pattern recognition, image processing, machine learning, granular computing, biometric authentication, and data fusion. Richa has more than 65 publications in refereed journals, book chapters, and conferences, and has received four best paper awards. She is a member of the IEEE, Computer Society, and ACM. She is also a member of Phi Kappa Phi, Tau Beta Pi, Upsilon Pi Epsilon, and Eta Kappa Nu honor societies.

Afzel Noore received his Ph.D. in Electrical Engineering from West Virginia University. He worked as a digital design engineer at Philips India. From 1996 to 2003, Dr. Noore served as the Associate Dean for Academic Affairs and Special Assistant to the Dean in the College of Engineering and Mineral Resources at West Virginia University. He is a Professor in the Lane Department of Computer Science and Electrical Engineering. His research interests include computational intelligence, biometrics, software reliability modeling, machine learning, hardware description languages, and quantum computing. His research has been funded by NASA, NSF, Westinghouse, GE, Electric Power Research Institute, the US Department of Energy, and the US Department of Justice. Dr. Noore has over 85 publications in refereed journals, book chapters, and conferences. He has received four best paper awards. Dr. Noore is a member of the IEEE and serves in the editorial boards of Recent Patents on Engineering and the Open Nanoscience Journal. He is a member of Phi Kappa Phi, Sigma Xi, Eta Kappa Nu, and Tau Beta Pi honor societies.