Dempster-Shafer Theory Based Classifier Fusion for Improved Fingerprint Verification Performance

Richa Singh[1], Mayank Vatsa[1], Afzel Noore[1], and Sanjay K. Singh[2]

[1] West Virginia University, Morgantown, WV - 26506, USA
{richas, mayankv, noore}@csee.wvu.edu
[2] Institute of Engineering and Technology, Jaunpur, UP 222001, India
sksiet@yahoo.com

Abstract. This paper presents a Dempster Shafer theory based classifier fusion algorithm to improve the performance of fingerprint verification. The proposed fusion algorithm combines decision induced match scores of minutiae, ridge, fingercode and pore based fingerprint verification algorithms and provides an improvement of at least 8.1% in the verification accuracy compared to the individual algorithms. Further, proposed fusion algorithm outperforms by at least 2.52% when compared with existing fusion algorithms. We also found that the use of Dempster's rule of conditioning reduces the training time by approximately 191 seconds.

1 Introduction

Fingerprint verification systems are widely based on minutiae and ridge information [1], [2]. Some algorithms use pattern information to recognize an individual [3]. Forensic experts rely on level-3 information such as pores and high level ridge information [4] for making a comparison. Further, many researchers have combined the outputs of two or more classifiers to improve the performance compared to a single classifier [5], [6], [7], [8]. The output of different classifiers can be fused at different levels such as image level, feature level, match score level, and decision level. However, fusing the output of different classifiers at match score level or at decision level makes the output independent of the type of classifier used.

Several different techniques such as sum rule [5], [6] and kernel based technique [8] have been proposed for biometric information fusion at match score or decision level. Most of these techniques rely on heuristic information extracted from the training data. Generally, these techniques do not update the priors regularly with the presence of new evidences, i.e. these techniques do not update the prior every time a new data is added in the database which is not pragmatic in high security applications. Another technique which is widely studied in classical classifier fusion but less addressed in biometrics is Dempster-Shafer (DS) theory [9], [10]. DS theory is a powerful method of combining accumulative evidences or for changing priors in the presence of new evidences. In [7], a match score fusion

P. Kalra and S. Peleg (Eds.): ICVGIP 2006, LNCS 4338, pp. 941–949, 2006.

algorithm is presented to fuse the information of face and voice using theoretic evidence of k-NN classifiers based on DS theory. Although authors have used DS theory, they did not use the conditioning scheme to regularly update the system based on new data. In this paper, four fingerprint verification algorithms; minutiae based [1], ridge based [2], fingercode based [3] and pores based [4] algorithms are used as different classifiers. Proposed Dempster-Shafer theory based fusion algorithm fuses decision induced match scores obtained from fingerprint verification algorithms. Further, conditioning algorithm is used to update the priors when new data is added in the database. On a fingerprint database obtained from different law enforcement agencies, experimental results show that the proposed algorithm is at least 2.52% better than the existing fusion algorithms. Section 2 presents an overview of DS theory and Section 3 presents the proposed classifier fusion algorithm. Section 4 shows the experimental results followed by conclusion in Section 5.

2 Overview of Dempster-Shafer Theory

Let Θ be a finite set of mutually exclusive and exhaustive proposition or commonly known as frame of discernment. The power set 2^{Θ} is the set of all subsets of Θ including itself and null set $\emptyset$. Each subset in the power set is called focal element. A value between [0, 1] is assigned to each focal element which is based on the evidence. 0 shows no belief and 1 shows total belief. Basic belief assignment (bba), in DS theory, is assigned to the individual proposition which is also known as mass of the individual proposition. It is assigned to every subset of the power set. If bba of an individual proposition A is $m(A)$ then,

$$\sum_{A \subset \Theta} m(A) = 1 \tag{1}$$

Also, bba of a null set is zero, i.e.

$$m(\emptyset) = 0 \tag{2}$$

Ignorance is represented by assigning the complementary probability to $m(\Theta)$. Measure of total belief committed to A, $Bel(A)$, is computed using Equation 3.

$$Bel(A) = \sum_{B \subset A} m(B) \tag{3}$$

According to Smets [10], formal notation of Bel is given as,

$$Bel_{Y,t}^{\Theta,\Re}[E_{Y,t}](\omega_o \in A) = x \tag{4}$$

This equation denotes the degree of belief x of the classifier Y at time t when ω_o belongs to set A, where A is the subset of Θ and $A \in \Re$; $\Re$ is a Boolean algebra of Θ. Belief is based on the evidential corpus $E_{Y,t}$ held by Y at time t where

$E_{Y,t}$ represents all what Y knows at time t. For simplicity $Bel_{Y,t}^{\Theta,\Re}[E_{Y,t}](\omega_o \in A)$ can be written as $Bel[E](A)$ or $Bel(A)$.

Plausibility function of A is defined as,

$$Pl(A) = 1 - Bel(\neg A) = \sum_{B \cap A \neq \emptyset} m(B) \tag{5}$$

$Bel(A)$ represents the lower limit of probability and $Pl(A)$ represents the upper limit. The difference between belief function and plausibility function represents the ignorance and $Bel(\Theta) = 1$, $Pl(\Theta) = 1$.

In most of the cases, it is required to update the belief based on new evidences or data. Let $E \subset \Theta$ and E_v be the evidence which states that the actual world is not in $\neg E$. Now suppose that the new data or evidence provides the exact value of E_v. Belief function is revised using the Dempster's rule of conditioning,

$$Bel[E_v](A) = Bel(A \cup \neg E) - Bel(\neg E) \tag{6}$$

Further, multiple evidences can be combined using Dempster's rule of combination. Let A and B be used for computing new belief function for the focal element C, Dempster's rule of combination is written as

$$m(C) = \frac{\sum_{A \cap B = C} m(A)m(B)}{1 - \sum_{A \cap B = \emptyset} m(A)m(B)} \tag{7}$$

3 DS Theory Based Classifier Fusion

In the proposed classifier fusion algorithm, DS theory [9], [10] is applied to combine the output of individual fingerprint verification algorithms to improve the verification performance shown in Figure 1. Minutiae based fingerprint verification algorithm [1], ridge based verification algorithm [2], fingercode based

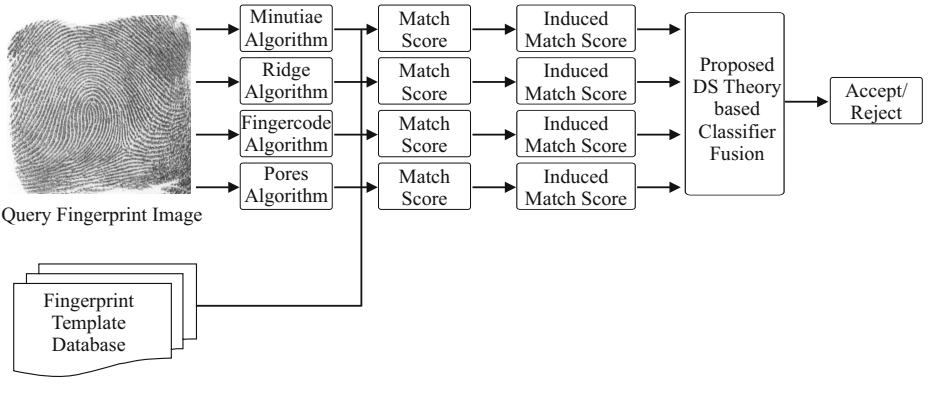

Fig. 1. Fusing the outputs of four fingerprint verification algorithms using proposed DS Theory based classifier fusion algorithm

verification algorithm [3] and pores based verification algorithm [4] are used as the primary classifiers. For every input fingerprint image, each classifier assigns a label true or 1 to proposition i, $i \in \Theta$ and the remaining classes are labeled as false or 0. Thus there are two focal elements for each fingerprint verification algorithm i and $\neg i = \Theta - i$. i is for confirming and $\neg i$ is for denying a single proposition for mass assignment in the DS theory. For every verification algorithm, we compute the respective predictive rates which are used to assign their bba. For a c class problem, let us assume that an input pattern belonging to class j ($j \in c$) be classified as one of the k ($k \in c+1$) classes including the rejection class, i.e. $(c+1)^{th}$ class. So, the predictive rate of a classifier P_k for an output class k is the ratio of the number of input patterns classified correctly to the total number of patterns classified as class k where input patterns belonging to all classes is presented to the classifier.

In the proposed approach, when the j^{th} fingerprint verification algorithm classifies the result $k \in (c+1)$ over the normalized matching score S_j, it is considered that for all instances the likelihood of k being the actual class is P_k and the likelihood of k not being the correct class is $(1-P_k)$. For the j^{th} fingerprint verification algorithm, first the decision induced match score is computed by multiplying P_{kj} with the respective normalized match score S_j. This score is then used as the basic belief assignment or mass $m_j(k)$ (Equation 8).

$$m_j(k) = P_{kj} \cdot S_j \tag{8}$$

where $j = 1, 2, 3, 4$, corresponds to the four fingerprint verification algorithms. Similarly disbelief is assigned to $m_j(\neg k)$; with $m(\Theta) = 1$. Further, mass of each evidence or classifier is combined recursively using Equation 9,

$$m_{final} = m_1 \oplus m_2 \oplus m_3 \oplus m_4 \tag{9}$$

where $\oplus$ shows the Dempster rule of combination. Since we are dealing with two class problem (true, false), we do not have to deal with the increasing computational complexity of DS theory [9]. Final result is obtained by applying threshold t to m_{final},

$$Result = \begin{cases} Accept, & if \quad m_{final} \geq t \\ Reject, & otherwise \end{cases} \tag{10}$$

Finally, the Dempster rule of conditioning given in Equation 6 is used to update the belief assignment associated with each fingerprint algorithm as and when required. With this rule, only new or updated bba is used for modification. This rule makes the update process easy as it is not required to train the complete classification algorithm when a new training data is added.

4 Experimental Results

Proposed DS theory based classifier fusion algorithm is validated using a fingerprint database obtained from different law enforcement agencies. The database contains five rolled fingerprints and five slap fingerprints from 500 different

classes. All the fingerprints are scanned at 1000 ppi. From each class, two rolled fingerprint images are randomly selected as training data. Rest of the images from each class are used as the test data. As stated earlier, minutiae based algorithm [1], ridge based algorithm [2], fingercode based algorithm [3] and pores based algorithm [4] are used as the primary classifiers. In the experiments, we compute the verification accuracy of all the algorithms at 0.001% false accept rate (FAR). Experimental results are divided into four subsections. In the first subsection, we compute the verification accuracies when test image is rolled fingerprint image, i.e. matching a rolled fingerprint with rolled fingerprint. In the next experiment, explained in Section 4.2, we compute the verification accuracies with slap fingerprints as the test images, i.e. matching rolled fingerprint with slap fingerprint. There are approximately 20 - 25 minutiae in a slap fingerprint which is less than the number of minutiae in rolled fingerprints (60 - 80 minutiae). Thus this experiment evaluates the performance when limited amount of information is present. The third experiment, which is the comparison of proposed fusion algorithm with existing fusion algorithms, is presented in Section 4.3. Finally, Section 4.4 presents the advantage of using Dempster rule of conditioning to reduce the training time.

4.1 Matching Rolled Fingerprints

For matching two rolled fingerprints using the four individual fingerprint verification algorithms, the best performance of 90.04% is obtained from minutiae based verification algorithm followed by 88.45% accuracy from pores based algorithm. Ridge and fingercode based algorithms give an accuracy of 84.61% and 85.39% respectively. Figure 2 shows the ROC plot of this experiment. It also shows that the verification accuracy of 98.14% is obtained when outputs of all the four verification algorithms are fused using the proposed DS theory based classifier fusion algorithm. Thus, the fingerprint verification performance is improved by 8.1%. Further, the verification accuracy of all the combinations of individual verification algorithms is computed by fusing the outputs of different verification algorithms using proposed fusion algorithm. Results are shown in Table 1. It shows that any combination with minutiae and pores based algorithms give better accuracy in comparison with other combinations.

4.2 Matching Rolled Fingerprint with Slap Fingerprint

In this experiment, the database images are rolled fingerprints and the testing dataset consists of slap fingerprints. Verification performance is computed for all combinations of four verification algorithms. Results of this experiment are shown in Table 2. It shows that the verification accuracy for all the combinations decreases by 2 - 3% in comparison to the verification accuracy of matching rolled to rolled fingerprints. In this experiment, fusion of outputs of all the four verification algorithms gives best result with 97.34% followed by fusion of minutiae and pores based algorithms with 95.85%.

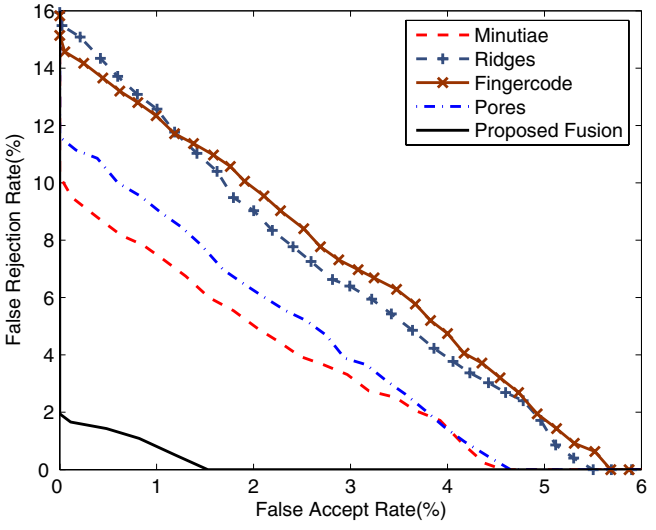

Fig. 2. ROC plot showing the performance of proposed fusion algorithm and individual fingerprint verification algorithms

Table 1. Verification accuracies of possible combinations using proposed fusion algorithm at 0.001% FAR (Matching rolled fingerprints)

Fusion Combination	Verification Accuracy
Minutiae + Ridges	94.70 %
Minutiae + Fingercode	94.66 %
Minutiae + Pores	96.43 %
Ridge + Fingercode	92.78 %
Ridge + Pores	93.89 %
Fingercode + Pores	93.56 %
Minutiae + Ridges + Fingercode	94.74 %
Minutiae + Ridges + Pores	96.07 %
Minutiae + Fingercode + Pores	95.69 %
Ridges + Fingercode + Pores	95.15 %
Minutiae + Ridges + Fingercode + Pores	**98.14** %

Further, we cropped the testing fingerprint images (slap fingerprints) such that no minutiae is present in the image with the constraint that the size of input testing image is 64×64. Using these images as testing images, we found that only pores based algorithm gives best performance with 87.93% whereas other verification algorithms give 0% accuracy. When the outputs are fused, any combination which includes the output of pores based algorithm give an accuracy of 87.93% and rest of the combinations give 0% verification accuracy. This experiment shows that with limited information pores based algorithm

Table 2. Verification accuracies of possible combinations using proposed fusion algorithm at 0.001% FAR with slap fingerprint images (Matching rolled fingerprints with slap fingerprints)

Fusion Combination	Verification Accuracy
Minutiae + Ridges	92.62 %
Minutiae + Fingercode	92.23 %
Minutiae + Pores	95.85 %
Ridge + Fingercode	90.46 %
Ridge + Pores	91.27 %
Fingercode + Pores	90.91 %
Minutiae + Ridges + Fingercode	93.12 %
Minutiae + Ridges + Pores	94.76 %
Minutiae + Fingercode + Pores	93.51 %
Ridges + Fingercode + Pores	94.08 %
Minutiae + Ridges + Fingercode + Pores	**97.34** %

is more useful and the proposed fusion algorithm is able to correctly fuse the outputs without compromising the verification performance.

4.3 Comparison with Existing Fusion Algorithms

In this experiment, a comparison of the proposed DS theory based classifier fusion algorithm with existing fusion algorithms is performed. For comparison, rolled fingerprint images are used as both training and testing images and fusion is performed with the outputs of minutiae and pores based algorithms only. Existing algorithms which are used for comparison are: Min/Max rule [5], Product rule [5], Sum rule [5], [6], and SVM fusion [8]. Figure 3 shows the ROC plot of this experiment. In this experiment, we found that Min/Max rule gives verification accuracy of 91.17%, product rule gives 92.01%, sum rule gives 92.76%, SVM fusion gives 93.91% whereas the proposed fusion algorithm outperforms these four fusion algorithms by at least 2.52% and gives an accuracy of 96.43%. This shows that the proposed fusion algorithm leads to greater improvement in performance compared to the other fusion algorithms.

4.4 Experiments with Dempster Rule of Conditioning

Another advantage of the proposed classifier fusion algorithm is low time complexity due to the Dempster's rule of conditioning. With this rule, the training time is reduced by splitting large dataset into smaller parts and updating mass assignments using the conditioning rule. Table 3 shows that when database size is 100, training time with and without conditioning rule is 245 seconds. This includes the time taken by four fingerprint verification algorithms and the proposed classifier fusion algorithm. When conditioning rule is not used, time required for training increases significantly with the increase in database size. However, the increment in time taken to train the database is much less when the conditioning

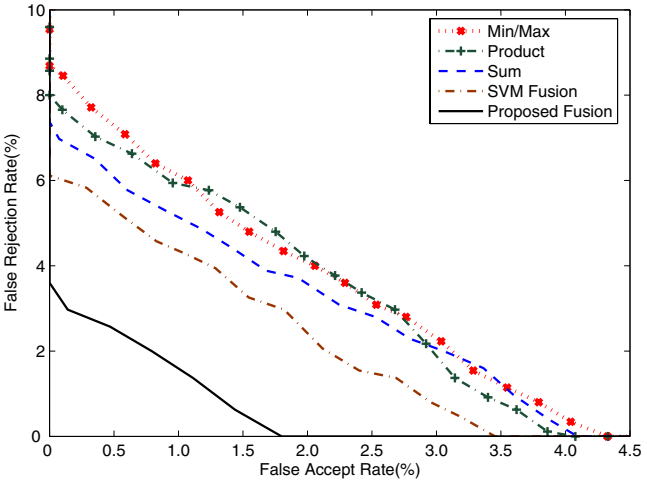

Fig. 3. ROC plot showing the performance comparison of proposed fusion algorithm with existing fusion algorithms

Table 3. Reducing training time of proposed fusion algorithm using Dempster's rule of conditioning

Database Size	Training time of fusion without conditioning (seconds)	Training time of fusion with conditioning (seconds)
100	245	245
200	459	392
300	631	538
400	829	685
500	1022	831

rule is used and is in the range of 146 - 147 seconds. This experiment shows that the use of conditioning algorithm can reduce the time complexity of fusion algorithm.

5 Conclusion

Improving the performance of fingerprint recognition algorithms is of paramount interest. In this paper, we proposed Dempster-Shafer theory based classifier fusion algorithm for improving fingerprint verification performance. Decision induced match scores of individual classifiers are used to compute the belief function in the DS theory based fusion algorithm. Further, multiple evidences are fused using Dempster's rule of combination. Four fingerprint algorithms are used as primary classifiers. Using a fingerprint database obtained from law enforcement agencies, verification accuracies of individual algorithms range from 84.61%

to 90.04%, whereas the proposed fusion algorithm gives an accuracy of 98.14% which is an improvement of around 8%. Further, performance of the proposed fusion algorithm is evaluated when limited information is presented and experimental results show that the proposed fusion algorithm is able to give consistent performance. A comparison of proposed fusion algorithm with existing fusion techniques is also performed, which demonstrates that the proposed fusion algorithm gives best results with 96.43% verification accuracy followed by SVM based fusion algorithm [8] with 93.91% accuracy. Finally, Dempster's rule of conditioning is used to reduce the time taken for training the database. Using this rule, time taken for training the database is reduced by approximately 191 seconds. This level of results shows the usefulness of proposed fusion algorithm for fingerprint recognition systems.

Acknowledgment

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.

References

1. Jain, A. K., Hong, L., Bolle, R.: On-line fingerprint verification. IEEE Transactions on PAMI. **19(4)** (1997) 302–314
2. Marana, A. N., Jain, A. K.: Ridge-based fingerprint matching using hough transform. Proceedings of Brazilian Symposium on Computer Graphics and Image Processing. (2005) 112–119
3. Jain, A. K., Prabhakar, S., Hong, L., Pankanti, S.: FingerCode: a filterbank for fingerprint representation and matching. Proceedings of IEEE Conference on CVPR. **2** (1999) 187–193
4. Kryszczuk, K., Drygajlo, A., Morier, P.: Extraction of level 2 and level 3 features for fragmentary fingerprints. Proceedings of the 2nd COST275 Workshop. (2004) 83–88
5. Kittler, J., Hatef, M., Duin, R. P., Matas, J. G.: On combining classifiers. IEEE Transactions on PAMI. **20(3)** (1998) 226–239
6. Ross, A., Jain, A. K.: Information fusion in biometrics. Pattern Recognition Letters. **24(13)** (2003) 2115–2125
7. Teoh, A., Samad, S. A., Hussain, A.: Nearest neighborhood classifiers in a bimodal biometric verification system fusion decision scheme. Journal of Research and Practice in Information Technology. **36(1)** (2004) 47–62
8. Aguilar, J. F., Garcia, J. O., Rodriguez, J. G., Bigun, J.: Kernel-based multimodal biometric verification using quality signals. Proceedings of SPIE Biometric Technology for Human Identification. **5404** (2004) 544–554
9. Shafer, G.: A mathematical theory of evidence. Princeton University Press 1976
10. Smets, P.: Decision making in a context where uncertainty is represented by belief functions. Belief Functions in Business Decisions (Srivastava, R., Mock, T. J. (ed.)) Physica-Verlag (2002) 17–61