DS theory based fingerprint classifier fusion with update rule to minimize training time

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

[1] *West Virginia University, Morgantown, WV 26506, USA*

[2] *Institute of Engineering and Technology, Jaunpur, 222001, India*

a) *noore@csee.wvu.edu*

Abstract: This paper presents a novel fingerprint classifier fusion algorithm using Dempster-Shafer theory concomitant with update rule. The proposed algorithm accurately matches fingerprint evidences and also efficiently adapts to dynamically evolving database size without compromising accuracy or speed. We experimentally validate our approach using three fingerprint recognition algorithms based on minutiae, ridges, and image pattern features. The performance of our proposed algorithm is compared with these individual fingerprint algorithms and commonly used fusion algorithms. In all cases, the proposed Dempster Shafer theory with update rule outperforms existing algorithms even with partial fingerprint image. We also show that as the database size increases, the proposed algorithm is designed to operate on only the augmented data instead of the entire database, thereby reducing the training time without compromising the verification accuracy.

Keywords: fingerprint recognition, classifier fusion, DS theory

Classification: Science and engineering for electronics

References

[1] A. K. Jain, L. Hong, and R. Bolle, "On-line Fingerprint Verification," *IEEE Trans. PAMI*, vol. 19, no. 4, pp. 302–314, 1997.

[2] A. N. Marana and A. K. Jain, "Ridge-Based Fingerprint Matching Using Hough Transform," *Proc. of BSCGIP*, pp. 112–119, 2005.

[3] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "FingerCode: A Filterbank for Fingerprint Representation and Matching," *Proc. of IEEE CVPR*, vol. 2, pp. 187–193, 1999.

[4] J. Kittler, M. Hatef, R. P. Duin, and J. G. Matas, "On Combining Classifiers," *IEEE Trans. PAMI*, vol. 20, no. 3, pp. 226–239, 1998.

[5] A. Teoh, S. A. Samad, and A. Hussain, "Nearest Neighborhood Classifiers in a Bimodal Biometric Verification System Fusion Decision Scheme," *J. Research and Practice in Inform. Tech.*, vol. 36, no. 1, pp. 47–62, 2004.

[6] J. F. Aguilar, J. O. Garcia, J. G. Rodriguez, and J. Bigun, "Kernel-Based Multimodal Biometric Verification Using Quality Signals," *Proc. of SPIE Biometric Technology for Human Identification*, vol. 5404, pp. 544–554,

DOI: 10.1587/elex.3.429
Received August 27, 2006
Accepted September 12, 2006
Published October 25, 2006

2004.

[7] P. Smets, "Decision Making in a Context where Uncertainty is Represented by Belief Functions," *Belief Functions in Business Decisions, R. Srivastava and T. J. Mock, (ed.)* Physica-Verlag, pp. 17–61, 2002.

1 Introduction

On-going research on improving fingerprint recognition accuracy has focused on several factors such as enhancing the quality of fingerprint during preprocessing, selecting different types of sensors for capturing fingerprints, developing matching algorithms based on different features, and using fusion techniques to combine matching scores or decisions. Also, the size of fingerprint database can affect the time taken to perform a match and hence can determine the acceptance of an algorithm for real-time applications. In this paper we address the scalability issue in the context of improving the accuracy of fingerprint recognition while keeping the overall matching time suitable for real-time application. We undertake this challenge by using three existing classifiers that perform fingerprint recognition based on minutiae [1], ridges [2], and image patterns [3]. Many researchers have combined the outputs of two or more classifiers to improve the performance compared to the performance of a single classifier [4, 5]. Fusing the output of different classifiers at match score level or at decision level makes the output independent of the type of classifier used. Furthermore, researchers have used different biometric information fusion techniques such as sum rule [4] and kernel based technique [6] to improve the performance. Most of these techniques rely on heuristic information extracted from the training data, and work well when the database is static. When the database evolves, the whole process has to be repeated on the entire database, resulting in lower performance.

This paper presents a classifier fusion approach based on Dempster-Shafer (DS) theory. DS theory is a powerful method of combining accumulative evidences or for changing priors in the presence of new evidences. In [5], a fusion 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 update scheme to regularly update the system based on new data. We propose Dempster-Shafer theory based classifier fusion algorithm using three fingerprint recognition algorithms [1, 2, 3]. The proposed fusion algorithm fuses the decision results of fingerprint recognition algorithms using their respective predictive rates. Unlike existing approaches, the uniqueness of this research is based on an update algorithm that operates only on augmented data instead of the entire cumulative data. The augmented data can represent varying information or evidence ranging from complete fingerprints of size 512 x 512 to cropped fingerprints of size 256 x 256 and 128 x 128. The algorithm is validated using a fingerprint database obtained from different law enforcement agencies. Experimental results show that the proposed algorithm takes lesser time for training and

DOI: 10.1587/elex.3.429
Received August 27, 2006
Accepted September 12, 2006
Published October 25, 2006

yields better accuracy compared to existing fusion algorithms.

2 Proposed Dempster Shafer Theory based Classifier Fusion

In the proposed classifier fusion algorithm, DS theory is applied to combine the output of individual fingerprint recognition algorithms to improve the verification performance. A brief overview of DS theory is given below.

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 the null set ϕ. Each subset in the power set is called focal element. Based on the evidence, a value between $[0, 1]$ is assigned to each focal element with 0 representing no belief and 1 representing total belief. Basic belief assignment (*bba*) is assigned to the individual propositions and is also known as the 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.

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

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

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

According to Smets [7], formal notation of *Bel* is given as,

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

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 $Bel^{\Theta,\Re}_{Y,t}[E_{Y,t}](\omega_o \in A)$ can be written as $Bel[E](A)$ or $Bel(A)$. Further, plausibility function of A is defined as,

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

$Bel(A)$ represents the lower limit of probability and $Pl(A)$ represents the upper limit.

Using the underlying concept to DS theory and basic belief assignment, classifier fusion is performed using minutiae based fingerprint recognition algorithm [1], ridge based recognition algorithm [2] and fingercode based recognition algorithm [3]. 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

© IEICE 2006
DOI: 10.1587/elex.3.429
Received August 27, 2006
Accepted September 12, 2006
Published October 25, 2006

recognition algorithm i and $\neg i = \Theta - i$. i is for confirming and $\neg i$ is for denying the proposition for mass assignment in the DS theory. For each fingerprint recognition algorithm, we compute the respective predictive rates used to assign their basic belief assignment. For a c class problem, let us assume that an input pattern belonging to class j $(j \in c)$ is 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 a fingerprint recognition algorithm classifies the result $k \in c+1$, 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 $(1 - P_k)$. The predictive rate is used as basic belief assignment or mass $m(k)$ and disbelief is assigned to $m(\neg k)$; with $m(\Theta) = 1$.

Further, multiple evidences are combined using the 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

$$m(C) = \frac{\sum\limits_{A \cap B = C} m(A)m(B)}{1 - \sum\limits_{A \cap B = \phi} m(A)m(B)} \tag{6}$$

Let m_1, m_2 and m_3 be the mass computed from the three fingerprint recognition algorithms or classifiers which are combined recursively as shown in Eq. (7),

$$m_{final} = m_1 \oplus m_2 \oplus m_3 \tag{7}$$

where $\oplus$ shows the Dempster's rule of combination. Final result is obtained by applying threshold t to m_{final},

$$result = \begin{cases} accept, & if \quad m_{final} \geq t \\ reject, & otherwise \end{cases} \tag{8}$$

2.1 Update Rule for Calculating Belief Assignment

In most 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 update rule,

$$Bel[E_v](A) = Bel(A \cup \neg E) - Bel(\neg E) \tag{9}$$

This rule is used to update the basic belief assignment associated with each fingerprint algorithm when a new training data is added. With this rule, only new basic belief assignments are used to update the classifier. The time required for updating is significantly less as it is not required to train the complete classification algorithm when new training data is added. Let m_1, m_2 and m_3 be the mass computed from the three fingerprint recognition

DOI: 10.1587/elex.3.429
Received August 27, 2006
Accepted September 12, 2006
Published October 25, 2006

algorithms or classifiers and m_1', m_2' and m_3' be the new basic belief assignments. If we represent the update rule with $\otimes$, then the updated basic belief assignments are represented as,

$$\begin{aligned} m_1^{update} &= m_1 \otimes m_1' \\ m_2^{update} &= m_2 \otimes m_2' \\ m_3^{update} &= m_3 \otimes m_3' \end{aligned} \tag{10}$$

3 Experimental Results

The proposed DS theory based fusion algorithm is validated using a fingerprint database obtained from different law enforcement agencies. The database contains five rolled and inked fingerprints from 200 different individuals. The size of each fingerprint is 512 x 512. One fingerprint from each individual is used as training data for minutiae based recognition algorithm [1], ridge based algorithm [2] and fingercode based algorithm [3]. The performance of the proposed algorithms is evaluated in terms of verification accuracy which determines if a query biometric template matches a stored reference template of an individual whose identity is being claimed. This is denoted by the percentage of correctly matched identities from all comparisons made. There are 800 genuine cases (200 x 4) corresponding to the same finger and 159,200 impostor cases (199 x 4 x 200) corresponding to different fingers that need to be verified. Table I shows the verification accuracy of the algorithms at 0.001% false accept rate (FAR).

Table I. Verification accuracy of fingerprint recognition algorithms and fusion algorithms at 0.001% FAR with varying image sizes

Image Size	Fingerprint Accuracy (%) using Different Algorithms							
	Minutiae [1]	Ridge [2]	Finger Code [3]	Sum Rule [4]	Min-Max Rule [4]	DS theory fusion [5]	Kernel based fusion [6]	Proposed DS classifier fusion with update rule
128 x 128	86.69	71.43	86.51	90.97	89.29	92.08	92.08	**95.58**
256 x 256	90.34	79.98	90.01	93.17	92.85	93.69	93.67	**96.14**
512 x 512	92.78	81.03	91.56	95.47	95.11	96.24	96.23	**97.01**

For the three fingerprint recognition algorithms, verification accuracies range from 81.03% to 92.78%. This table also shows performance comparison of the proposed DS theory based fusion algorithm with four existing fusion algorithms, sum rule [4], min-max rule [4], DS theory based match score fusion algorithm [5] and kernel based fusion algorithm [6]. The proposed DS theory based classifier fusion algorithm gives an accuracy of 97.01% which is 0.77% better than the previously proposed DS theory based match score fusion algorithm [5]. Table I also shows that the proposed fusion algorithm leads to greater improvement in performance compared to other fusion algorithms.

DOI: 10.1587/elex.3.429
Received August 27, 2006
Accepted September 12, 2006
Published October 25, 2006

Further, we highlight the advantage of the proposed DS theory based fusion algorithm when the evidence is limited. We performed experiments to evaluate the performance of the proposed algorithm with varying fingerprint information. In this experiment, we reduced the size of fingerprint images by cropping with respect to center of the fingerprint images. In this manner we created two sets of fingerprint databases: one with size 256 x 256, and another with size 128 x 128. We evaluated the performance of all eight algorithms on these databases. The first two rows of Table I show the results for this experiment. With 128 x 128 size fingerprint database, the proposed algorithm gives an accuracy of 95.58% which is at least 3.50% better than other algorithms. Similarly, with 256 x 256 size database, the improvement is 2.45%. These results clearly indicate that the proposed fusion algorithm outperforms other algorithms even with partial fingerprint information.

Another advantage of the proposed classifier fusion algorithm is the reduction in time complexity due to the update rule. With this rule, the training time is reduced by splitting large dataset into smaller parts and updating the mass assignment. Table II shows that when the database size is 40, the training time with and without update rule is 110 seconds. This includes the time taken by the fingerprint recognition algorithm and the proposed classifier fusion algorithm. When update rule is not used, the training time increases significantly with the increase in database size. However, when the update rule is used the training time is significantly less.

Table II. Reducing training time of proposed fusion algorithm using update rule

Database Size	Training time of fusion without update rule (seconds)	Training time of fusion with update rule (seconds)
40	110	110
80	198	141
120	261	176
160	329	204
200	374	232

4 Conclusion

In this paper, we present a novel fingerprint classifier fusion algorithm using Dempster Shafer theory with update rule to improve the performance of fingerprint recognition. In the proposed fusion algorithm, decisions obtained from standard fingerprint recognition algorithms are fused along with their respective predictive rates. We also propose the use of Dempster's update rule to update the classifier by operating only on augmented data. Experimental results show that the proposed fusion algorithm outperforms other fusion algorithms even with reduced fingerprint information. The results also show that the use of Dempster's update rule on the new or augmented data reduces the training time without compromising accuracy.

DOI: 10.1587/elex.3.429
Received August 27, 2006
Accepted September 12, 2006
Published October 25, 2006

Acknowledgments

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.

DOI: 10.1587/elex.3.429
Received August 27, 2006
Accepted September 12, 2006
Published October 25, 2006