Fuzzy Fusion Filter for Multi-Modal Biometric Systems

Holger Findling, *Senior Member, IEEE*

Abstract—Research has shown that performances of biometric identification systems can be enhanced with multi-modal fusion. Incorporating prescreening and filtering feature vector files stored in repositories are necessary steps to realize required speed performances. We propose the application of a fuzzy fusion filter to the prescreening stages of a multi-modal identification system to enhance the throughput and reliability of the overall system. This paper evaluates the design and performances of a generic fuzzy fusion filter.

Index Terms— Multi-Modal Biometric Systems, Fusion, Fuzzy Expert Systems.

1 Introduction

In 1924 the FBI Identification Division was established with a collection of 810,000 fingerprint cards [1]. Identification of subjects was a manual process conducted by fingerprint experts; the need for computer automation became a natural progression with an increase in size of the fingerprint repository and the number of searches required. The Integrated Automated Fingerprint Identification System (IAFIS) went operational in July 1999 with a fingerprint repository in excess of 40 million subjects. The success of this system created much interest by many commercial and government institutions, where all share a common need for automated biometric identification systems with requirements that include high reliability and very fast throughput rates.

Biometric identification systems differ greatly from biometric verification systems in regard to the size of the search space and the quality of extracted feature vectors. In a biometric verification system the quality and orientation of fingerprints and facial features can be controlled. However, in a biometric identification system the orientation and quality of extracted feature vectors can vary considerably; furthermore, it can be difficult to remove a latent fingerprint from the physical background, which may also contain patterns.

Biometric identification systems can be classified as either uni-modal or multi-modal identification systems. Uni-modal identification systems, using either fingerprint identification or facial feature recognition are limited, because system reliability becomes a function of the size of the repositories and the accuracy of the algorithms. Research has shown that the False Match Rate (FMR) increases linearly with the increase in size of the repository [2]. Multi-modal biometric systems have been shown to improve system performances. Recently, much research interest has developed in this field, including fusion of various modalities [3], [4], [5]. Figure 1 shows a multi-modal biometric identification system that uses two modalities – facial recognition [6], [7], [8] and fingerprint matching [9], [10]. Latent fingerprints and facial images, which were obtained from a crime scene, are processed to potentially find a matching template in the repository. Since latent fingerprints are typically comprised of few minutiae, facial feature vectors (if available) can be used to enhance the search and greatly reduce the search space.

The Fuzzy Fusion Filter is a critical component of this system, enabling a fast throughput rate while maintaining high reliability. In the fusion process the scores obtained from the facial-feature matching algorithm and the fingerprint prescreen algorithm are fused together to produce a list of subjects which is passed on to the final fingerprint matching stage. The fingerprint prescreen algorithm [11] is extremely fast (less than 350 µsec), but by itself is not reliable enough to make a complete identification. Combining the results with the facial recognition scores reduces the subjects in the fingerprint repository to less than 2 percent, thereby greatly reducing the workload on the final fingerprint matching stage.

2 Fusion

Fusion of data can be performed at various stages in a multi-modal identification system. Common fusion techniques can be characterized as combining attribute fusion, decision fusion, and voting fusion [4]. The purpose of these fusion methods is to improve reliability by elevating the matching template to the top position. The combining attribute method utilizes a conglomerate feature vector, created from feature vectors containing attributes from all modes, in a single identification algorithm. Decision fusion mathematically merges match scores generated by individual classifiers (related to attributes) into a single weighted score, implying the rank or probability of identification. During voting fusion, a ranking (decision) is assigned to each entry, with final ranking based on the majority of output decisions [4]. The Fuzzy Fusion Filter is most closely identified with decision fusion, although its purpose is to produce a subset of subjects from the repository that includes the matching template.

3 Fuzzy Fusion Filter

The design of a fuzzy expert system does not require that a mathematical expression relate input variables to output va-

riables. Fuzzy expert systems generate solutions from approximate information instead of bivalent propositional associations. Input variables applied to fuzzy logic are not limited to discrete values. Instead, the variables can assume any value in the interval of zero to one.

During the fuzzification process the matchscores of the different classifiers can easily be normalized to fit into the fuzzy interval. One method to normalize match scores is to divide the scores by the highest match score, which is produced by matching the search template with itself.

Once the matchscores are fuzzified, the fuzzy system must perform a transformation from input fuzzy sets to output fuzzy sets. A collection of rules is referred to as the knowledgebase or rule base of the system. These rules determine how the Fuzzy Fusion Filter S maps input fuzzy sets, I^n, to output fuzzy sets, I^p. I^n is comprised of the input universe of discourse, $N = \{n_1, \ldots n_r\}$, and I^p is comprised of the output universe of discourse $P = \{p_1, \ldots, p_r\}$. S performs the transformation shown in equation 1, and is characterized as a fuzzy associative memory (FAM) [13].

$$S : I^n \rightarrow I^p \tag{1}$$

The Fuzzy Fusion Filter receives two input values – one input from the facial feature matching algorithm and the other value from the fingerprint prescreen algorithm. The fuzzification process determines the degree of membership in the possible input fuzzy sets, I^n. Each input value can hold full membership in any of the eight triangles T_1 through T_8, in either trapezoid, T_0 or T_9, as shown in Figure 2, or partial membership in any two adjacent geometric figures. All base angles are 45 degrees and the adjacent sides overlap 50 percent; this arrangement ensures that no data distortion occurs and total membership in I^n sums to 1.0.

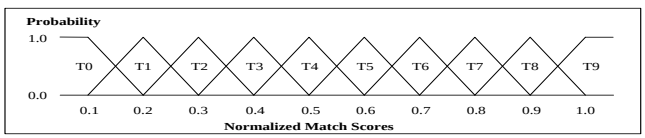

Figure 2. Fuzzification

The Fuzzy Fusion Filter output B defined in equation (2) is shown as being comprised of 100 fuzzy sets in Figure 3. w_m is the weight of the rules that map I^n to I^p, and represents the degree of membership in the output fuzzy sets. w_i is determined by the product correlation inference and can be scaled by the ratio of the reliabilities of the two classifiers used. A classifier with greater reliability should be given more weight then a weaker cassifier. B is the resultant of all activated output fuzzy sets. Equation (2) illustrates that each entry into the FAM matrix maps to at least one output fuzzy set, $w_i B_i$. However the total possible number of activated output fuzzy sets in B is limited to four, since all partial memberships in the input fuzzy sets are limited to any two adjacent geometric figures.

$$B = w_1 \cdot B_1 + \ldots + w_m \cdot B_m \tag{2}$$

The FAM matrix in Figure 3 shows crisp values for each fuzzy output set B_i. Although a mathematical relationship is not required to map input fuzzy sets to output fuzzy sets, the entries were derived from the Euclidian distance of the fuzzy input intervals. These values can be heuristically changed to optimize the performance of the system. In accordance with Figure 3, values for fuzzy output sets $T_{(0,0)}$ through $T_{(4,4)}$ are set to 0.000, since the probability of identification is below 50%, and considered unreliable. Any additional processing for this candidate template can be terminated; the feature vectors of the search template do not match the candidate template.

Set 1

T9	1.004	1.019	1.044	1.077	1.118	1.166	1.220	1.280	1.345	1.414
T8	0.905	0.921	0.948	0.984	1.029	1.081	1.140	1.204	1.272	1.345
T7	0.806	0.824	0.854	0.894	0.943	1.000	1.063	1.131	1.204	1.280
T6	0.707	0.728	0.761	0.806	0.860	0.921	0.989	1.063	1.140	1.220
T5	0.608	0.632	0.670	0.721	0.781	0.848	0.921	1.000	1.081	1.166
T4	0.000	0.000	0.000	0.000	0.000	0.781	0.860	0.943	1.029	1.118
T3	0.000	0.000	0.000	0.000	0.000	0.721	0.806	0.894	0.984	1.077
T2	0.000	0.000	0.000	0.000	0.000	0.670	0.761	0.854	0.948	1.044
T1	0.000	0.000	0.000	0.000	0.000	0.632	0.728	0.824	0.921	1.019
T0	0.000	0.000	0.000	0.000	0.000	0.608	0.707	0.806	0.905	1.004
Set 2	**T0**	**T1**	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**

Figure 3. FAM Matrix

In the Fuzzy Fusion Filter the defuzzification process converts the fuzzy output sets into a single crisp output value; and this step can be combined with composition into one process. The composition process creates output fuzzy set B, which requires defuzzification to provide for a normalized output value Z:

$$Z = \frac{B}{T_{(9,9)}} \tag{3}$$

4 TEST DATA

The reliability of a biometric identification system is dependent on the size of the repository and accuracy of the classifiers used. In order to test the Fuzzy Fusion Filter, a large repository of fingerprint feature vectors and associated facial feature vectors is needed. Due to the difficulties of obtaining such large correlated data sets, normalized match scores for one hundred candidates and 15,000 subjects were created using a Durham-Shuffle random generator. The synthesized data sets were first created with 100 percent reliability by inserting the highest match scores into the candidates' match score position. Additional data sets were then adjusted to produce reliabilities within a range of 50 to 90 percent.

When the reliability of the data sets was adjusted below 100 percent, candidate match scores were randomly selected to be included in the top 1500 ranks and below the top 15 rank. For example, a data set with 70 percent reliability has 30 percent of the candidate match scores in the top 1500 ranks and below

the top 15 ranks. As indicated by Figure 4, for each classifier, 100 sets of 15,000 normalized match scores were created for testing purposes.

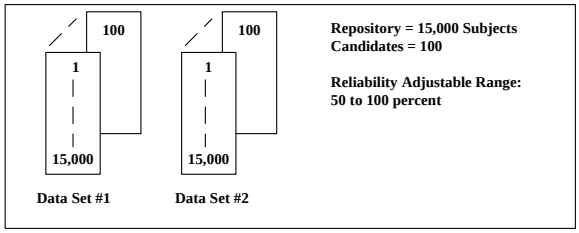

Figure 4. Test Data

Since the normalized match scores were created with a random generator, the distribution of these scores produced an equal number of entries in each fuzzy input set. Therefore, the data sets have one hundred percent reliability at a ten percent filter rate. The candidate match scores were also adjusted to produce data sets with one hundred percent reliability at a 20 percent filter rate. This implies that the matching candidate is included in the top 3000 ranking positions versus the 1500 ranking positions for the 10 percent filter rate.

5 RESULTS

The fuzzy fusion algorithm was tested with five different data sets, each representing one hundred candidates matched against 15,000 subjects. The five data sets varied in reliability from 50 to 90 percent, however all matching candidates were included in the top 1500 ranks. The test results are shown in Tables 1 through 5, where the reliability of each data set is shown in respect to the filter rates.

Table 1 shows that Set 1 and Set 2 are 50 percent reliable at a 0.1 percent filter rate. This implies that 50 percent of the time a matching candidate was found in the top 15 ranking position per search against the repository. Set 1 represents the results of the facial feature matching algorithm and Set 2 represents the results of the fingerprint presceen algorithm. The Fusion column shows the results of the Fuzzy Fusion Filter applied to Set 1 and Set 2.

Table 1- 50 % Reliability

Filter Rate	Set 1	Set 2	Fusion
0.1	50	50	41
0.5	52	52	83
1.0	53	53	93
2.0	**55**	**55**	**100**
3.0	60	64	100
5.0	65	73	100
10.0	100	99	100
20.0	100	100	100
30.0	100	100	100

Table 2- 60 % Reliability

Filter Rate	Set 1	Set 2	Fusion
0.1	60	60	58
0.5	61	60	86
1.0	62	62	99
2.0	**70**	**65**	**100**
3.0	86	82	100
5.0	99	100	100
10.0	100	100	100
20.0	100	100	100
30.0	100	100	100

Table 3- 70 % Reliability

Filter Rate	Set 1	Set 2	Fusion
0.1	70	70	64
0.5	72	71	90
1.0	73	73	99
2.0	**76**	**74**	**100**
3.0	78	79	100
5.0	86	85	100
10.0	99	99	100
20.0	100	100	100
30.0	100	100	100

Table 4- 80 % Reliability

Filter Rate	Set 1	Set 2	Fusion
0.1	80	80	77
0.5	80	80	95
1.0	**80**	**82**	**100**
2.0	82	84	100
3.0	87	88	100
5.0	100	94	100
10.0	100	100	100
20.0	100	100	100
30.0	100	100	100

Table 5- 90 % Reliability

Filter Rate	Set 1	Set 2	Fusion
0.1	90	90	89
0.5	90	90	96
1.0	91	90	99
2.0	**91**	**90**	**100**
3.0	93	92	100
5.0	96	95	100
10.0	99	100	100
20.0	100	100	100
30.0	100	100	100

The results suggests that the output of the Fuzzy Fusion Filter generates subsets of subjects that are one hundred percent reliable at a filter rate of 2 percent, when the score of the matching template ranks in the top 10 percent. This implies that only 300 subjects need to be evaluated in the final matching stage instead of the 15,000 subjects stored in the repository. If the matching template is contained in the repository, it is also included in the subset.

Additional tests were conducted with data sets having one hundred percent reliability at a twenty percent filter rate. Table 6 shows the results for classifiers having 70 percent reliability. The fused data is one hundred percent reliable at a five percent filter rate. A decrease of three percent in the filter rate is realized when the matching template score is ranked in the top twenty percent versus the top ten percent. It is highly unlikely that the final matching stage could elevate a matching template to the top position when the prescreen stages show the subject in the 750^{th} place. Performance differences in processing latent fingerprints between the fingerprint prescreen algorithms and fingerprint matching algorithms are not great enough to significantly realize the required improvements in matching capabilities to elevate a subject with a low rank in the prescreen stage.

Table 6- 70 % Reliability

Filter Rate	Set 1	Set 2	Fusion
0.1	70	70	61
0.5	70	71	74
1.0	70	71	81
2.0	72	72	95
3.0	74	75	97
5.0	**79**	**77**	**100**
10.0	87	86	100
20.0	100	100	100
30.0	100	100	100

5.1 Complexity Analysis

The Fuzzy Fusion Filter algorithm executes the fuzzification, inference, and defuzzification process for each search template matched against a template stored in the repository. The fuzzification process requires execution of a maximum of 22 conditional statements, assigning memberships in fuzzy input sets. This process is independent of the size of the repository and can be performed in constant time. The inference process can be implemented with a for-loop instead of using if-then conditional statements. Inference requires determining variable w_i which maps input fuzzy sets to one hundred fuzzy output sets. Since the size of the FAM matrix is fixed, inference can be executed in constant time. Defuzzification is the only process that requires a division operator, and the normalization of data is applied to the FAM matrix in constant time. The fuzzy expert system worst case running time, $O(n)$, is a linear function of the size of the repository, n.

The output scores of the fuzzy expert system must be sorted by rank to determine the top percentile of subjects. Subjects with scores below a cutoff threshold can be discarded before sorting, thereby minimizing execution cost. Sorting is performed in $O(n \cdot \lg(n))$ and represents the highest cost in the Fuzzy Fusion Filter implementation.

6 Conclusion

We introduced in this paper, a novel fuzzy fusion filter, and showed its feasibility for improving performances of multi-modal biometric identification systems. Experimental Results, using one hundred search candidates and two large repositories (15,000 templates each), indicate that the search space can be reduced to two percent of the repository size while maintaining 100 percent reliability. Therefore, using multi-modalities and a fuzzy fusion filter to minimize the search space reduces processing costs typically associated with the rigorous matching algorithms in the final stage.

An advantage of using the fuzzy fusion filter algorithm is its ease of adaptability to different biometric modalities. In comparison to statistical based fusion filters, the fuzzy fusion filter has a very low running cost and does not require a large memory space to store prescreen match scores. The FAM matrix used for the inference in the Fuzzy Fusion Filter algorithm can be easily adjusted to compensate for differences in the characteristics of the biometric modalities used. Adjustments for differences in reliability for the biometric modalities can also be implemented directly in the fuzzy filter, instead of adjusting the normalized match scores in the fuzzification process. This capability allows optimizing the matching performance and throughput rates of the biometric system.

Future biometric identification systems will require much greater throughput rates to meet demands of new emerging global economies, homeland security, and law enforcement. To accomplish higher throughput rates prescreen algorithms must be fast and can't sacrifice in reliability; however computational speed and reliability of classifiers are not complementary. Fingerprint prescreen algorithms and fuzzy fusion filters are very fast in comparison to facial feature matching algorithms [14, 15]. Much research is still needed to develop faster prescreen algorithms and indexing for reducing the search space of facial feature vectors.

It should be noted that the final identification is greatly dependent on the accuracy of the final matching stage. Fusion algorithms can enhance the performance of multi-modal biometric identification systems, but should not be used to compensate for weak classifiers.

Acknowledgment

The authors wish to thank the PhD Student Organization at the Florida Institute of Technology for helpful discussions and contributions to the Fuzzy Fusion Filter algorithm.

REFERENCES

[1] *The Science of Fingerprints,* United States Department of Justice, FBI (Rev. 12-84), 1980.

[2] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition,* Springer, 2003, ISBN: 0-387-95431-7.

[3] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification," *IEEE Transactions on Neural Networks,* vol. 10, no. 5, pp. 1065-1074, Sep. 1999.

[4] S.A. Israel, W.T. Scruggs, W.J. Worek, and J.M. Irvine, R.H. Walden, "Fusing Face and ECG for Personal Identification," *Proc. Of 32nd Applied Imagery Pattern Recognition Workshop (AIPR '03*), Oct. 2003.

[5] L. Hong and A.K. Jain, "Integrating Faces and Fingerprint for Personal Identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 20, no. 12, pp. 1295-1307, Dec. 1998.

[6] R.K. Sadykhov, V.A. Samokhval, and L.P. Pedenok, "Face Recognition Algorithm on the Basis of Truncated Walsh-Hadamard Transform and Synthetic Discriminant Functions," *IEEE Proc. of the Sixth International Conference on Automatic Face and Gesture Recognition (FGR '04)*, pp. 219-212, May 2004.

[7] J.L.Kostantinos, N. Plataniotis, and A.N. Venetsanopoulos, "Face Recognition Using LDA-Based Algorithms," *IEEE Transactions on Neural Networks,* vol. 14, no. 1, pp. 195-200, Jan. 2003.

[8] C. Liu and H. Wechsler, "Evolutionary Pursuit and Its Application to Face Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 22, no. 6, pp. 570-582, Jun. 2000.

[9] G.S. Ng, X. Tong, X. Tang, and D. Shi, "Adjacent Orientation Vector Based Fingerprint Minutiae Matching System," *IEEE Proc. of the 17th International Conference on Pattern Recognition (ICPR '04)*, vol. 1, pp. 528-531, Aug. 2004.

[10] H. Selvaraj, S. Arivazhagan, and L. Ganesan, "Fingerprint Verification Using Wavelet Transform," P*roc. of the Fifth International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2003)*, pp. 430-435, Sep. 2003.

[11] S. Prabhakar, A.K. Jain, J.Wang, S. Pankanti, and R. Bolle, "Minutiae Adjacent Orientation Vector Based Fingerprint Minutia Verification and Classification for Fingerprint Matching," *Proc. of the 15th International Conference on Pattern Recognition*, vol. 1, pp. 25-29, Sep. 2000.

[12] A.R. Sanders, J.F. Curtis, and H. Findling, *Finger Print Matching System with ARG-Based Prescreener*, U.S. Patent 6,778,687, Aug. 2004.

[13] B. Kosko, *Neural Networks and Fuzzy Systems*, Prentice Hall, 1992, ISBN: 0-13-611435-0.

[14] A.K. Jain, L. Hong, Y. Kulkarni, "F2ID: A Personal Identification System Using Faces and Fingerprints," *Proc. of the Fourteenth International Conference on Pattern Recognition,* vol. 2, pp. 1373-1375, Aug. 1998.

[15] R Feraud, O.J. Bernier, J. Viallet, and M. Collobert, "A Fast and Accurate Face Detector Based on Neural Networks," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 1, pp. 42-53, Jan 2001.

Holger Findling is a senior member of IEEE and received the BSEE degree from the University of Central Florida in 1986, the M.S.M. in Contract Management, 1989, and the MSCS degree, 1996, from the Florida Institute of Technology. He joined Information Systems, Lockheed Martin Corporation in 1997 and worked for the Automated Fingerprint Identification System (AFIS) program. His research interest is in algorithm design of biometric systems. He is teaching as an Adjunct Professor at the Orlando Graduate Center, Florida Institute of Technology.