Biometric Fusion: Robust Approach

Oleg Ushmaev, Sergey Novikov
BioLink Technologies
OUshmaev@biolinkusa.com, SNovikov@biolink.ru

Abstract

We have developed biometric fusion technique based on stochastic theory. The suggested method is a robust adaptation of the Neyman-Pearson technique to the specifics of biometrics. The method makes possible to achieve almost optimal performance as measured by the ROC curve.

1. Introduction

As of today, biometric technologies are replacing other person authentication methods in a great scope of applications [1-13]. It is caused by at least three reasons:

- demands to information resources protection require hardening of traditional passwords
- increasing power of computers allows to implement biometric technologies in real time applications
- states allocate sufficient funds on biometric programs due to necessity of improvement of border security and law enforcement effectiveness.

The main criteria of quality of a biometric technology are recognition rates: probability of the false rejection (False Rejection Rate, FRR) and probability of the false acceptance or false alarm in watch list applications (False Acceptance Rate, FAR).

The results of biometric testing show [3,10,14-21] that none of existing single biometics (even iris or fingerprint) meets strict requirements to the recognition rates in number of applications such as civil ID, border security, law enforcement etc. In addition each single biometrics may not be convenient or even available. In view of this, the multimodal biometrics seems to be the most effective way to achieve better performance. The general scheme of multimodal biometric system is presented in the figure 1.

Integration of muliple biometrics modalities has two aspects: technical and algorithmic. Technically, the biometric fusion is designing united interface for a number of separate biometric systems or applications. This problem has been successfully solved by standardization.

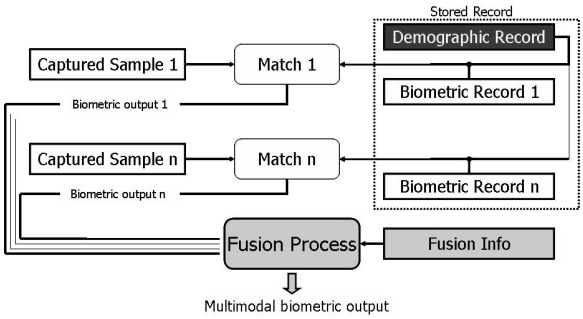

Figure 1 – Biometric fusion scheme

From the algorithmic point of view, succesfull integration of different biometric modalities is rather complicated mathematical task.

Apparent, and somewhat "standard" [4], way to create an optimal (that provides the best performance as measured by ROC) multimodal output is an applying Neyman-Pearson theorem [25]. The essence of the theorem is: the optimal numerical criterion is the ratio of the simultaneous probability density in genuine matches over the probability density in impostor matches

However, the direct applying of this precise mathematical technique is absolutely impractical. The keystone of the Neyman-Pearson approach is the accurate estimation of the score probability densities [31], that usually requires reasonable training data.

The apparent p.d.f. estimations are the empiric densities. But small size of available training sets of biometric samples makes empiric probability densities being absolutely unreliable estimation of score pdf, especially in genuine matches. That is why successful applying of Neymann-Pearson theorem requires sufficient adaptaion of p.d.f. estimation technique to the specifics of biometrics.

The second major problem is verification of the fusion results. Often multimodal biometrics are aimed to achieve acceptable FRR when FAR is extremely low (less than 10^{-6}). In that case the fusion performance can not be verified during technological or operational testings due to unavailability of the biometric samples database of the proper size. It demands from fusion methods robustness and possibility of forecasting the FRR for extremely low levels of the FAR.

We suggest approach to estimation of pdf based on the integral robust parameters estimated from empiric biometric data. The paper is organized as follows. The mathematical methods of robust biometric fusion are presented in section 2. The results of experiments are in section 3.

2. Algorithms

2.1. General approach

Theoretically, given score vector **s** distributions f_{gen} in genuine matches and f_{imp} in impostor matches, optimal similarity criterion s_{opt} can be calculated as logarithm of ratio of the probability density in genuine matches over the probability density in impostor matches:

$$s_{opt} = \ln f_{gen}(\mathbf{s}) - \ln f_{imp}(\mathbf{s}). \qquad (1)$$

In practice, the probability densities can be estimated as empiric densities obtained in a technological testing. However, designing multimodal system one has to take into account that empiric densities are not reliable estimation of the score pdf. Confidential interval for empiric densities is about $1/\sqrt{N}$, where N – number of matches [23].

We suggest that empiric densities can be substituted by score distributions moments of several initial orders. Moments are more robust and integral characteristic of score distributions than p.d.f. Given values of score moments, score pdf can approximated by a distribution with same moments from some parameterized class. Similar approach to pdf estimation is widely used in stochastic systems theory [23]. Particularly pdf is approximated by functions of the following sort:

$$f_k(\mathbf{s}) = P_k(\mathbf{s}) g_{\mathbf{m},\mathbf{K}}(\mathbf{s}), \qquad (2)$$

where $P_k(\mathbf{s})$ is a polynom of degree *k*, **m** – the score average, **K** – the score covariation matrix, *g* – basic distribution function with first moments close to **m** and **K**. In spirit of central limit theorem, it is worth taking density of Gaussian distribution as basic function g, as far as great number of parameters affect biometric output that makes score distribution close to some weighted mixture of gaussians.

The polynom $P_k(\mathbf{s})$ coefficients are calculated under assumption that the moments $\mathrm{M}_{\mathrm{emp}}^{j_1 \ldots j_n}$ of observed score distribution are equal to the moments $\mathrm{M}_{\mathrm{par}}^{j_1 \ldots j_n}$ of distribution with density (2). If $P_k(\mathbf{s})$ is written in the following form:

$$P_k(\mathbf{s}) = \sum \alpha_{i_1 \ldots i_n} s_1^{i_1} \ldots s_n^{i_n} \qquad (3)$$

then equations for moments can be written as:

$$\begin{aligned} \mathrm{M}_{\mathrm{par}}^{j_1 \ldots j_n} &= \int s_1^{j_1} \ldots s_n^{j_n} P_k(\mathbf{s}) g(\mathbf{s}) ds_1 \ldots ds_n = \\ &\sum \int s_1^{j_1} \ldots s_n^{j_n} \alpha_{i_1 \ldots i_n} s_1^{i_1} \ldots s_n^{i_n} g(\mathbf{s}) ds_1 \ldots ds_n = \\ &= \sum \alpha_{i_1 \ldots i_n} \mathrm{M}^{i_1 + j_1 \ldots i_n + j_n}[g(\mathbf{s})] = \mathrm{M}_{\mathrm{emp}}^{j_1 \ldots j_n}, \end{aligned} \qquad (4)$$

where $\mathrm{M}^{i_1 + j_1 \ldots i_n + j_n}[g(\mathbf{s})]$ are known moments of basic distribution. Coefficients $\alpha_{i_1 \ldots i_n}$ are found as solution of system of linear equations (4) for moments of order less or equal to *k*.

Once theoretical estimations of probability densities have been calculated, theoretical recognition rates can be evaluated using either analytical or Monte Carlo approaches.

2.2. Independent biometrics fusion

Examples of independent biometrics are fingerprint and face, face and voice etc. From the pure mathematical point of view, an independence of different biometrics cannot be proved. But at the same time there is no sense considering absolutely different biometrics (like face and finger) being statistically dependent at the technological level (some dependencies might be observed on operational level due to such factors as unfriendly interface or inadequate user behavior).

The distinguishing feature of independent biometrics is the decomposition of the simultaneous probability densities:

$$\begin{aligned} f_{imp}(\mathbf{s}) &= f_{imp}^1(s_1) \ldots f_{imp}^n(s_n) \\ f_{gen}(\mathbf{s}) &= f_{gen}^1(s_1) \ldots f_{gen}^n(s_n) \end{aligned} \qquad (5)$$

For an arbitrary index *i*, p.d.f. in genuine and impostor matches can be approximated with Gaussian distribution:

$$\hat{f}(s) = c e^{-\frac{(s-m)^2}{2\sigma^2}}. \qquad (6)$$

The gaussain approximation does not always fit well real distribution. More complicated distributions can be approximated using the method of moments (section 2.1) by the following function [23]:

$$f(s;k)=\frac{P_k(s)}{\sqrt{2\pi}\sigma}e^{-\frac{(s-m)^2}{2\sigma^2}}, \qquad (7)$$

where $P_k(s)$ is polynom of degree k, m – the score average, σ – the standard deviation of score.

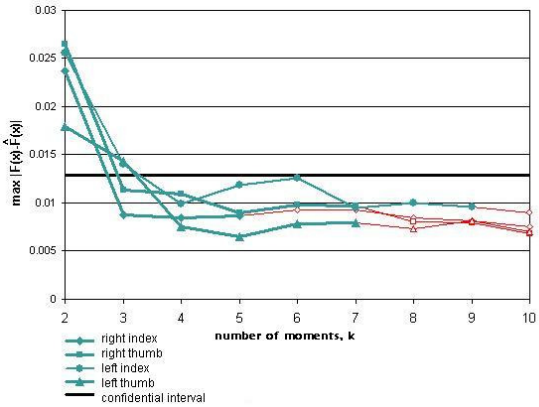

Figure 2 – Approximation of probability densities

Although function (7) depends on very few parameters (several moments of initial orders), the proposed method gives reasonably good approximation of pdf.

The results of experiments with approximation of score distributions are presented in figure 2. The examples of real biometric scores were taken from a protocol of the technology testing of the Biolink algorithm on NIST SD 14. As an index of quality of approximation, maximal difference between the empiric density and the estimation (7) is taken. The graph shows that the densities estimated by the suggested method are located in the confidential interval for real pdf. In particular, it means that the density (7), based on a small number of parameters, provides not worse approximation of the real pdf than the empiric density.

After the score distributions in genuine and impostor matches are approximated with functions like (7), the optimal score can be calculated as:

$$S_{\text{opt}}(s)=\ln P_{gen,k}(s)-\ln P_{imp,m}(s)-\ln\left(\sqrt{2\pi}\sigma_{gen}\right)+ \\ +\ln\left(\sqrt{2\pi}\sigma_{imp}\right)-\frac{(s-m_{gen})^2}{2\sigma_{gen}^{\ 2}}+\frac{(s-m_{imp})^2}{2\sigma_{imp}^{\ 2}}, \qquad (8)$$

overall optimal score is:

$$S_{\text{opt}}(\mathbf{s})=\ln f_{gen}(\mathbf{s})-\ln f_{imp}(\mathbf{s})= \\ =\sum_i \ln f^i_{gen}(s_i)-\ln f^i_{imp}(s_i)=\sum_i S^i_{opt}(s_i) \qquad (9)$$

As the formula (9) shows, a biometric output can be standardized in such a way that fusion process of independent biometrics becomes the simple summation. Schematically the fusion of independent biometrics is presented in the figure 3 where the standard biometric output satisfies the equation:

$$s=\ln\frac{f_{gen}(s)}{f_{imp}(s)}. \qquad (10)$$

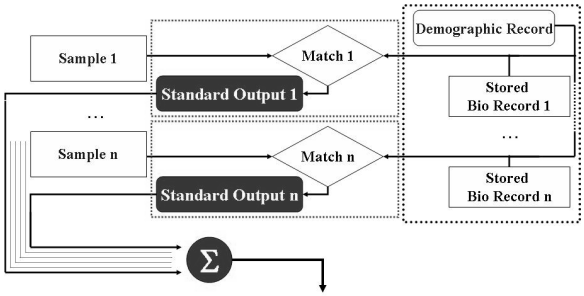

Figure 3 – Scheme of the independent biometrics fusion

2.3. Dependent biometrics fusion

Generally the dependent biometrics fusion can be implemented like the independent biometric fusion (section 2.2). However, additional correlations between the different modalities must be taken into account. Similarly to (7) densities might be estimated as:

$$f(\mathbf{s};k)=\frac{P_k(\mathbf{s})}{(2\pi)^{n/2}|\mathbf{K}|}e^{-\frac{(\mathbf{s}-\mathbf{m})\mathbf{K}^{-1}(\mathbf{s}-\mathbf{m})^T}{2}}. \qquad (11)$$

Parameters of basic (gaussian) distribution are estimated from the score average vector and the covariation matrix.

3. Experiments

3.1. Fusion of independent biometrics

As example of the independent biometric fusion, the fusion of the Cognitec facial and the Biolink fingerprint recognition algorithms were considered. The input data about the score distribution for face algorithm were obtained from results of technology testing FRVT 2002[27]. Fingerprint algorithm score distributions were taken from NIST VTB[16] analytical report, published in 2003. We used three initial moments for estimation of probability densities both in genuine and impostor matches.

The theoretical performance of designed bimodal algorithm are presented in figure 4. As one can see the fusion greatly improves recognition performance. Unfortunately these results cannot be verified as far as no database with both face and finger samples of enough size is public available.

Purely fusion performance can be measured on Biometric Score Sets Release 1 (BSSR1) database [29]. Preliminary the BSSR1 subset was randomly divided into two subsets: training and testing to demonstrate both effectiveness and robustness of the proposed approach. The results of applying of the proposed fusion technique to fing_x_face subset (216 samples) of BSSR1 are presented in figure 5. Markers show the fusion algorithm performance for different divisions of the BSSR1 score .

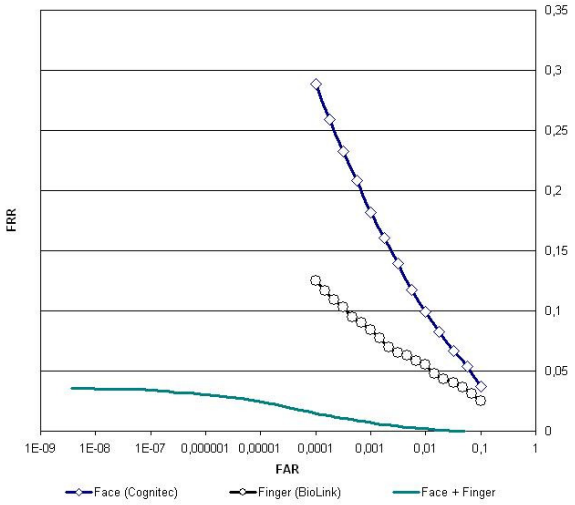

Figure 4 – ROC of face and finger algorithms

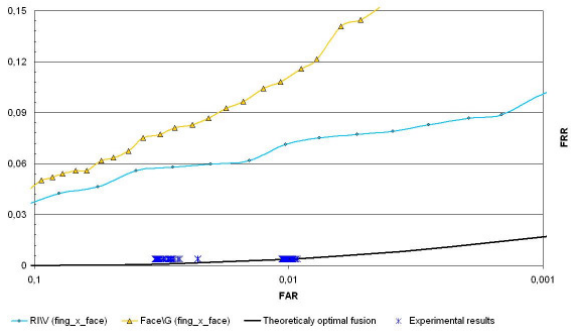

Figure 5 – Fusion performance on BSSR1

3.2. Fusion of dependent biometrics

Fusion of dependent biometrics is complicated by correlation between matching results. In experiments we combined scores for different fingers.

The correlation between scores are presented in tables below [28]. We took results of the Biolink algorithm [27] on NIST SD 14 tenprints database [26].

As one can see genuine scores are moderately correlated. We approximated score pdf using 2 initial moments of simultaneous distributions, i.e. totally 20 numbers. Fusion performance for two and four-finger solutions are presented in figure 6. The optimal score is referred as IS1. The IS2 graphs show results of direct applying of the independent biometric fusion technique (without registration of correlations) to the multifinger fusion. Slight difference between the IS1 and IS2 graphs demonstrates that the registration of correlations improves the recognition performance even for weakly correlated biometrics.

Correlations in impostor matches

	Right Index	Right Thumb	Left Index	Left Thumb
Right Index	1.00000	0.00174	0.00411	0.00176
Right Thumb	0.00174	1.00000	0.00171	0.00405
Left Index	0.00411	0.00171	1.00000	0.00211
Left Thumb	0.00176	0.00405	0.00211	1.00000

Correlations in genuine matches

	Right Index	Right Thumb	Left Index	Left Thumb
Right Index	1.000	0.312	0.290	0.262
Right Thumb	0.312	1.000	0.298	0.349
Left Index	0.290	0.298	1.000	0.287
Left Thumb	0.262	0.349	0.287	1.000

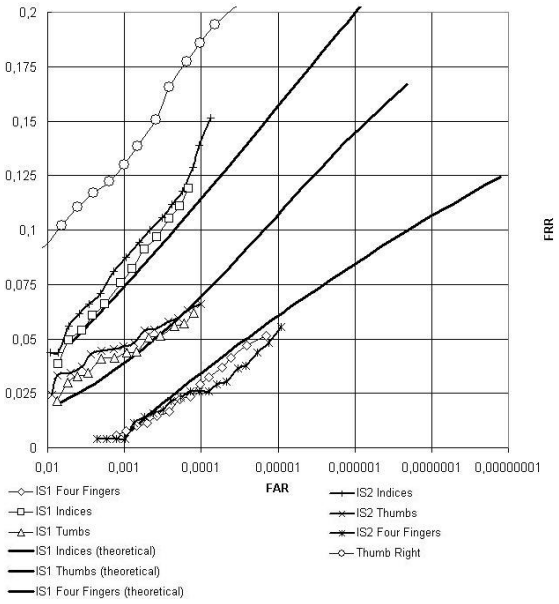

Figure 6 – The ROC of the multifinger algorithms

The results of experiments also reveal good compliance between the theoretical and empiric recognition rates of the multifinger algorithms. So theoretical ROC might be used to forecast the behavior of the acqured multifinger solutions at low FAR.

3.3. Multi-algorithms fusion

Multialgorithm fusion is the most challenging case of biometric fusion. Different algorithms might have extremely high score correlations. But at the same time, the integration of multiple algorithms is the cheapest way of technology improvement. For demonstration of multialgorithm fusion performance, we took the two different fingerprint recognition algorithms. The first was the BioLink minutiae based algorithm referred as Biolink MST at NIST FpVTE (not adapted for small capture area of capacity live scanners). The second algorithm was an experimental correlation based algorithm. As a testing set, FVC2002 DB3 was chosen. Both the genuine and impostor densities were estimated using three initial moments of score distributions [31].

The ROC of separate and combined algorithms are presented in Figure 7.

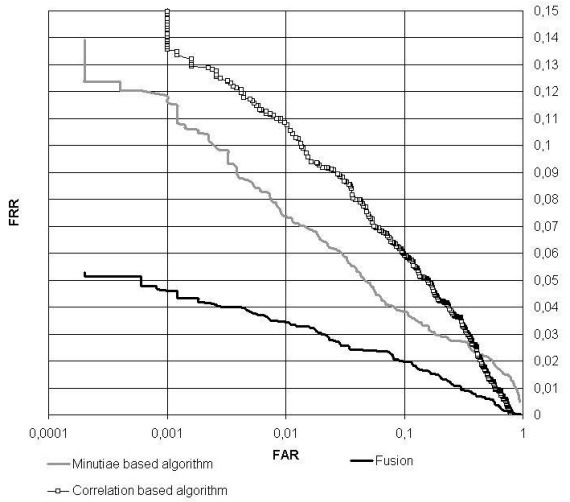

Figure 7 – The multialgorithm fusion performance

4. Conclusions

The proposed fusion technique based on stochastic theory allows to achieve almost the best possible performance measured as ROC curve. Sufficient advantages of the method are:

- robustness to small training sets that is typical problem of biometric fusion
- possibility to make fusion process fully automatic.

At the same time the proposed approach slows down multimodal biometric system, since it requires simultaneous availability of matching scores for all biometric systems. Apparently biometric fusion can successfully solve the problem of increasing of throughput of multimodal systems (for example, tenprint matching algorithms are as fast as or even faster than one fingerprint algorithms).

Designing of fusion process simultaneously optimizing recognition rates and throughout of multimodal biometric systems is a task for the further research.

6. References

[1] Federal Bureau of Investigation, “The FBI Fingerprint Identification Automation Program: Issues and Options”, U.S. Government Publication, U.S. Congress, Office of Technology Assessment, Washington, DC, 1991.

[2] N. Kingsbury, Technology Assessment: Using Biometrics for Border Security. DIANE Publishing Co., 2003.

[3] James Wayman et al. Biometric Systems: Technology, Design and Performance Evaluation. Springer Verlag, 2004.

[4] P. Griffin, “Topics for Multi-Biometrics Research” // Panel Discussion MMUA’2003. http://mmua03.cs.ucsb.edu

[5] Jain A.K., Hong L., Pankanti S. and Bolle R., “An Identity-Authentication System Using Fingerprints”, *Proc. of IEEE*, 1997, 85(9), pp. 1365-1388.

[6] Daugman J., “The Importance of Being Random”, *Pattern Recognition*, vol.36, no.2, 2003.

[7] Daugman J., Recognizing Persons by Their Iris Patterns, in Biometrics: Personal Identification in a Networked Society, A.K. Jain, R.Bolle, and S.Pankanti (edt.), Kluwer Academic, New York, 1999.

[8] Halici U., Jain L.C., Erol A., Introduction to Fingerprint Recognition, Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999.

[9] John D. Woodward, Jr. “Biometrics: Facing Up to Terrorism”, The Biometric Consortium Conference 2002, Arlington, February, 2002.

[10] Beardsley, Chartles T., Is your computer insecure?, IEEE Spectrum, Jan, 1972, pp.67-78.

[11] Federal Bureau of Investigation, "The Science of Fingerprints: Classifications and Uses", U.S. Government Publication, Washington, DC, 1984.

[12] Jain A.K., Hong L. and Bolle R., "On-Line Fingerprint Verification", *IEEE Trans. On Pattern Analysis and Machine Intelligence*, 1997, 19(4), pp. 302-314.

[13] Biometrics in Driver's License Operations. http://www.biometricgroup.com/dl_id_operations.pdf

[14] First International Competition for Fingerprint Verification Algorithms (FVC2000), http://bias.csr.unibo.it/fvc2000/.

[15] FVC2002, the Second International Competition for Fingerprint Verification Algorithms (FVC2002), http://bias.csr.unibo.it/fvc2002/.

[16] "Studies of Fingerprint Matching Using the NIST Verification Test Bed (VTB)" available at ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7020.pdf

[17] Face Recognition Vendor Test, http://www.frvt.org

[18] Fingerprint Vendors Technology Evaluation, http://fpvte.nist.gov

[19] T. Mansfield et al. "Biometric Product Testing Final Report". UK Biometrics Working Group, 2001, http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf

[20] A.J. Mansfield and J.L. Wayman "Best Practices in Testing and Reporting Performance of Biometric Devices". UK Biometrics Working Group, 2002.

[21] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar. Handbook of Fingerprint Recognition. Springer Verlag, New York, 2003

[22] ANSI INCIST 358-2002.

[23] Pugachev V.S., Sinitsin I.N., Stochastic Systems. Theory and Applications. Singapore, World Scientific, 2001.

[24] Frischholz R.W., Dieckmann U., "BioID: A Multimodal Biometric Identification System", IEEE Computer, pp. 64-68, Feb. 2000.

[25] Neyman J. and E.S. Pearson (1933) On the problem of the most efficient tests of statistical hypotheses. Philos. Trans. Roy. Soc., London A, 231, p. 289-337.

[26] C.Watson, NIST Special Database 14: Mated Fingerprint Card Pairs 2, CD-ROM & documentation, September 1993.

[27] U.S. Patent No. 6282 304.

[28] O. Ushmaev and S. Novikov, Integral Criteria for Large-scale Multiple Fingerprint Solutions // SPIE Symposium on Security & Defense. Orlando, FL, USA, April 12-16, 2004.

[29] NIST Biometric Scores Set – Release 1 (NIST BSSR1), http://www.itl.nist.gov/iad/894.03/biometricscores/

[30] Richard O. Duda, Peter E. Hart, Pattern Classification and Scene Analysis. – John Wiley & Sons, New York, 1973.

[31] O. Ushmaev "Biometric fusion: methods, algorithms" PhD thesis, 2004.