An Integrated Approach for Automated Authentication Based On Multimodal Biometric System

Devireddy Srinivasa Kumar

ABSTRACT

Biometrics refers to the automatic identification of an individual based on his/her physiological or behavioral traits. Unimodal biometric systems perform person recognition based on a single source of biometric information and are affected by problems like noisy sensor data, non-universality and lack of individuality of the chosen biometric trait. Some of the limitations imposed by unimodal biometric systems (that is, biometric systems that rely on the evidence of a single biometric trait) can be overcome by using multiple biometric modalities. Such systems, known as Multimodal biometric systems, are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence. A multimodal biometric system integrates information from multiple biometric sources to compensate for the limitations in performance of each individual biometric system. An optimal framework for combining the matching scores from multiple modalities using the likelihood ratio statistic computed using the generalized densities estimated from the genuine and impostor matching scores is being proposed in this paper. The motivation for using generalized densities is that some parts of the score distributions can be discrete in nature; thus, estimating the distribution using continuous densities may be inappropriate. The two approaches for combining evidence based on generalized densities: (i) the product rule, which assumes independence between the individual modalities, and (ii) copula models, which consider the dependence between the matching scores of multiple modalities are being presented in this paper.

Dept. of CSE&IT, Nalanda Institute of Engineering & Technology,Kantepudi - 522438, Guntur

1. INTRODUCTION

Traditionally Passwords (Knowledge based Security) and ID cards (token-based security) have been used to restrict access to secure systems. However, security can be easily breached in these systems when a password is revealed to an unauthorized user or a card is stolen by an impostor. Furthermore, simple passwords are easy to guess by an impostor and difficult passwords may be hard to recall by a legitimate user. The emergence of biometrics has addressed the problems that plague traditional verification methods. Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person. Current biometric systems make use of fingerprints, hand geometry, iris, retina, face, facial thermo grams, signature, gait, palm print and voiceprint to establish a person's identity.

While biometric systems have their limitations they have an edge over traditional security methods, in that they cannot be easily stolen or shared. Besides strengthening the security, biometric systems also enhance user convenience by reducing the need to design and remember passwords. Moreover, biometrics is one of the few techniques that can be used for negative recognition where the system determines whether the person is who

he or she denies to be. Biometric systems can operate in one of two modes—the identification mode, in which the identity of an unknown user is determined, and the verification mode, in which a claimed identity is either accepted (a genuine user) or rejected (an impostor). Biometric systems are being deployed in various applications including computer logins, ATMs, grocery stores, airport kiosks, and driver's licenses. The successful installation of biometric systems in these applications does not imply that biometrics is a solved problem. In fact, there is significant room for improvement in biometrics as suggested by the error rates shown in the table-1. Biometric systems installed in real-world applications must contend with a variety of problems. Among them are:

i) Noise in sensed data. A fingerprint with a scar and a voice altered by a cold are examples of noisy inputs. Noisy data could also result from defective or improperly maintained sensors (for example, accumulation of dirt on a fingerprint sensor) and unfavorable ambient conditions (for example, poor illumination of a user's face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.

ii) Intra-class variations. The biometric data acquired from an individual during authentication may be very different from the data used to generate the template during enrollment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor, or when sensor characteristics are modified (for example, by changing sensors, that is, the sensor interoperability problem) during authentication.

iii) Distinctiveness. While a biometric trait is expected to vary significantly across individuals, there may be large similarities in the feature sets used to represent these traits. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.

iv) Non-universality. While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users to not possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of the ridges. Thus, there is a Failure To Enroll (FTE) rate associated with using a single biometric trait. There is empirical evidence that about 4% of the population may have poor quality fingerprints that cannot be easily imaged by some of the existing sensors.

v) Spoof attacks. An impostor may attempt to spoof the biometric trait of a legitimately enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioral traits such as signature and voice are used. However, physical traits like fingerprints are also susceptible to spoof attacks.

Table 1 : State-of-the-art error rates associated with fingerprint, face and voice biometric systems.

Biometric Type	Test	Test Parameter	False Reject Rate (FRR)	False Accept Rate (FAR)
Fingerprint	FVC 2002	Users mostly in the age group 20-39.	0.2%	0.2%
Face	FRVT 2002	Enrolment and test images were collected in varied lighting, outdoor/ indoor environment and could be on different days	10%	1%
Voice	NIST 2000	Text dependent	10-20%	2-5%

Biometrics refers to the automatic identification of an individual based on his/her physiological traits [1]. Biometric systems based on a single source of information (unimodal systems) suffer from limitations like the lack of uniqueness, non-universality and noisy data [2] and

hence, may not be able to achieve the desired performance requirements of real-world applications. Some of the limitations imposed by unimodal biometric systems (that is, biometric systems that rely on the evidence of a single biometric trait) can be overcome by using multiple biometric modalities. Such systems, known as Multimodal biometric systems, are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence. Multimodal biometric systems have several advantages over unimodal systems. Combining the evidence obtained from different modalities using an effective fusion scheme can significantly improve the overall accuracy of the biometric system. A multimodal biometric system can reduce the Failure to Enroll (FTE)/ Failure to Capture (FTC) rates and provide more resistance against spoofing because it is difficult to simultaneously spoof multiple biometric sources. Multimodal systems can also provide the capability to search a large database in an efficient and fast manner. This can be achieved by using a relatively simple but less accurate modality to prune the database before using the more complex and accurate modality on the remaining data to perform the final identification task. However, multimodal biometric systems also have some disadvantages. They are more expensive and require more resources for computation and storage than unimodal biometric systems. Multimodal systems generally require more time for enrollment and verification causing some inconvenience to the user. Finally, the system accuracy can actually degrade compared to the unimodal system if a proper technique is not followed for combining the evidence provided by the different modalities. However, the advantages of multimodal systems far outweigh the limitations and hence, such systems are being increasingly deployed in security-critical applications. These systems are also able to meet the stringent performance requirements imposed by various applications. Multi biometric systems address the problem of non-universality, since multiple traits can ensure sufficient population coverage. Furthermore, multimodal biometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. By asking the user to present a random subset of biometric traits, the system ensures a live user is indeed present at the point of data acquisition. Thus, a challenge-response type of authentication can be facilitated using multi biometric systems. A variety of factors should be considered when designing a multi biometric system. These include the choice and number of biometric traits; the level in the biometric system at which information provided by multiple traits should be integrated; the methodology adopted to integrate the information; and the cost versus matching performance trade-off. The choice and number of biometric traits is largely driven by the nature of the application, the overhead introduced by multiple traits (computational demands and cost, for example), and the correlation between the traits considered. In a cell phone equipped with a camera it might be easier to combine the face and voice traits of a user, while in an ATM application it might be easier to combine the fingerprint and face traits of the user. In a multimodal biometric system, integration can be done at (i) feature level, (ii) matching score level, or (iii) decision level. Matching score level fusion is commonly preferred because matching scores are easily available and contain sufficient information to distinguish between a genuine and an impostor case. Given a number of biometric systems, one can generate matching scores for a pre-specified number of users even without knowing the underlying feature extraction and matching algorithms of each biometric system. Thus, combining information contained in the matching scores seems both feasible and practical.

This paper proposes a framework for optimally combining the matching scores from multiple modalities based on generalized densities estimated from the genuine and impostor matching scores. The motivation for using generalized densities is that some parts of the score distributions can be discrete in nature. As a result, estimating the densities using continuous density functions can be inappropriate. This paper presents two approaches for combining evidence based on generalized densities: (i) the product rule, which assumes independence between the individual modalities, and (ii) copula models, which parametrically model the dependence between the matching scores of multiple modalities. The proposed method bypasses the need for score normalization and selection of optimal weights for the score combination on a case-by-case basis [3, 9], and therefore, is a more principled approach with performance comparable to the commonly used fusion methods.

2 Generalized Densities

2.1 Estimation of Marginal Distributions

Let X be a generic matching score with distribution function F, i.e., $P(X \leq x) = F(x)$. We denote the genuine (impostor) matching score by X_{gen} (X_{imp}) and the corresponding distribution function by f_{gen} (f_{imp}). Assuming that $f_{gen}(x)$ and $f_{imp}(x)$ have densities $f_{gen}(x)$ and $f_{imp}(x)$, respectively, the Neyman-Pearson theorem states that the optimal ROC curve is the one corresponding to the likelihood ratio statistic $NP(x) = f_{gen}(x)/f_{imp}(x)$ [10]. The ROC curve corresponding to $NP(x)$ has the highest Genuine Accept Rate (GAR) for every given value of the False Accept Rate (FAR) compared to any other statistic $U(x) \neq NP(x)$ (this is true even for the original matching scores corresponding to $U(x) = x$). However, when $f_{gen}(x)$ and $f_{imp}(x)$ are unknown (which is typically the case) and are estimated from the observed matching scores, the ROC corresponding to $NP(x)$ may turn out to be suboptimal. This is mainly due to the large errors in the estimation of $f_{gen}(x)$ and $f_{imp}(x)$. Thus, for a set of genuine and impostor matching scores, it is important to be able to estimate $f_{gen}(x)$ and $f_{imp}(x)$ reliably and accurately. Previous studies by Griffin [10] and Prabhakar et al. [11] assume that the distribution function F has a continuous density with no discrete components. In reality, most matching algorithms apply thresholds at various stages in the matching process. When the required threshold conditions are not met, specific matching scores are output by the matcher (e.g., some fingerprint matchers produce a score of zero if the number of extracted minutiae is less than a threshold). This leads to discrete components in the matching score distribution that cannot be modeled accurately using a continuous density function. A score value x_0 is said to be discrete if $P(X = x_0) = p > 0$. It is easy to see that F cannot be represented by a density function in a neighborhood of x_0 (since this would imply that $P(X = x_0) = 0$). Thus, discrete components need to be detected and modeled separately to avoid large errors in estimating $f_{gen}(x)$ and $f_{imp}(x)$. Our approach consists of detecting discrete components in the genuine and impostor matching score distributions, and then modeling the observed distribution of matching scores as a mixture of discrete and continuous components. Hence, this approach generalizes the work of [10,11]. The following methodology can model a distribution based on a generic set of observed scores. For a fixed threshold T, the discrete values are identified as those values x_0 with $P(X = x_0) > T$, where $0 \leq T \leq 1$. Since the underlying matching score distribution is unknown, we estimate the probability $P(X = x_0)$ by $N(x_0)/N$, where $N(x_0)$ is the number of observations in the data set that equals x_0, and N is the total number of observations. The collection

of all discrete components for a matching score distribution will be denoted by

$$D \equiv \left\{ x_0 : \frac{N(x_0)}{N} > T \right\} \quad (1)$$

The discrete components constitute a proportion $PD \equiv \sum_{x_0 \in D} \frac{N(x_0)}{N}$ of the total observations. We obtain the collection C by removing all discrete components from the entire data set. The scores in C constitute a proportion $PC \equiv 1 - PD$ of the entire data set, and they are used to estimate the continuous component of the distribution $(F_C(x))$ and the corresponding density $(f_c(x))$. A non-parametric kernel density estimate of $f_c(x)$ is obtained from C as follows. The empirical distribution function for the observations in C is computed as

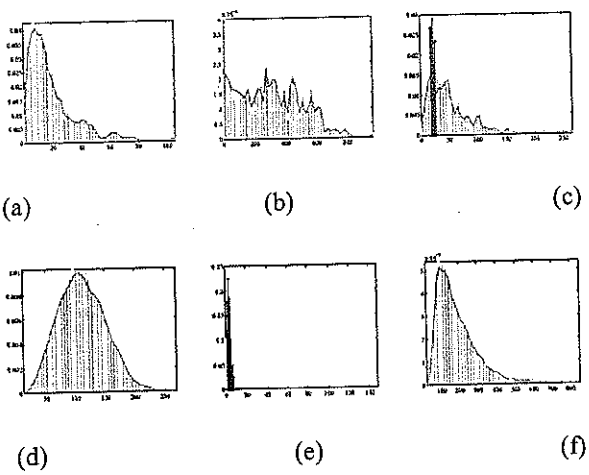
$$F_C(x) = \frac{1}{N_C} \sum_{s \in C} I\{s \le x\} \quad (2)$$

where $I\{s \le x\} = 1$ if $s \le x$, and $= 0$, otherwise; also, $N_C \equiv N_{PC}$. Note that $F_C(x) = 0 \; \forall \; x < s_{min}$ and $F_C(x) = 1 \; \forall \; x \ge s_{max}$, where s_{min} and s_{max}, respectively, are the minimum and maximum of the observations in C. For values of x, $s_{min} < x < s_{max}$, not contained in C, $F_C(x)$, is obtained by linear interpolation. Next, B samples are simulated from $F_C(x)$, and the density estimate of $f_C(x)$, $f_c(x)$, is obtained from the simulated samples using a Gaussian kernel density estimator. The optimal bandwidth, h, is obtained using the "solve-the-equation" bandwidth estimator [12], which is an automatic bandwidth selector that prevents over smoothing and preserves important features of the distribution of matching scores. The generalized density is defined as

$$l(x) = pc\, fc(x) + \sum_{x_0 \in D} \frac{N(x_0)}{N} I\{x = x_0\} \quad (3)$$

where $I\{x = x_0\} = 1$ if $x = x_0$, and $= 0$, otherwise. The distribution function corresponding to the generalized density is defined as

$$L(x) = pc \int_{-\infty}^{x} fc(u)\,du + \sum_{x_0 \in D, x_0 \le x} \frac{N(x_0)}{N} \quad (4)$$



(a) (b) (c)

(d) (e) (f)

Fig 1: Histograms of genuine scores for face (a), finger (b), and hand-geometry (c).

Histograms of impostor scores for face (d), finger (e), and hand-geometry (f).

For a multimodal system with K modalities, the generalized densities and distributions estimated for the genuine (impostor) scores for the k^{th} modality will be denoted by $l_{gen,k}(x)$ and $L_{gen,k}(x)$ ($l_{imp,k}(x)$ and $L_{imp,k}(x)$), respectively, for $k = 1, 2, \ldots, K$. Figures 1 (a)-(f) give the plots of $l_{gen,k}(x)$ and $l_{imp,k}(x)$ for the distribution of observed genuine and impostor matching scores for $K = 3$ modalities of the EXP-Multimodal database (see Section 4). Figures 1 (a)-(f) also give the histograms of the genuine and impostor matching scores for the three modalities. The "spikes" (see Figure 1 (c) and (e)) represent the detected discrete components and have a height greater than the threshold $T = 0.02$. Note that the individual "spikes" cannot be represented by a continuous density function. Forcing a continuous density estimate for these values will result in gross estimation errors and yield suboptimal ROC curves.

2.2 Joint Density Estimation using Copula Models

The methodology described in Section 2.1 only estimates the marginal score distributions of each of the K modalities without estimating the joint distribution. One way to estimate the joint distribution of matching scores is by using copula models [13]. Let $H_1, H_2, ..., H_K$ be K continuous distribution functions on the real line and H be a K-dimensional distribution function with the k^{th} marginal given by H_k for $k = 1, 2, ..., K$. According to Sklar's Theorem [13], there exists a unique function $C(u_1, u_2, ..., u_K)$ from $[0, 1]^K$ to $[0,1]$ satisfying

$$H(s_1, s_2, ..., s_K) = C(H_1(s_1), H_2(s_2), ..., H_k(s_k)) \quad (5)$$

where $s_1, s_2, ..., s_K$ are K real numbers. The function C is known as a K-copula function that "couples" the one-dimensional distributions functions $H_1, H_2, ..., H_K$ to obtain the K-variate function H. Equation (5) can also be used to construct K-dimensional distribution functions H whose marginals are the distributions $H_1, H_2, ..., H_K$: choose a copula function C and define H as in (5).

Copula functions are effective in modeling the joint distribution when the marginal distributions are non-normal and do not have a parametric form (as is usually the case for biometric data). The family of copulas considered in this paper is the K-dimensional multivariate Gaussian copulas [14]. These functions can represent a variety of dependence structures using a K x K correlation matrix R. The K-dimensional Gaussian copula function with correlation matrix R is given by

$$C_R^K(u_1, u_2, ..., u_k) = \Phi_R^K(\Phi^{-1}(u_1), \Phi^{-1}(u_2), ..., \Phi^{-1}(u_K)) \quad (6)$$

where each u_k [0,1] for $k = 1, 2, ..., K$, $\Phi(\bullet)$ is the distribution function of the standard normal, $\Phi^{-1}(.)$ is its inverse, and Φ_R^K is the K-dimensional distribution function of a random vector $Z = (Z_1, Z_2, ..., Z_K)^T$ with component means and variances given by 0 and 1, respectively. The $(m,n)^{th}$ entry of R, ρ_{mn}, measures the degree of correlation between the m-th and n-th components for $m, n = 1, 2, ..., K$. In practice, $\hat{A}_{mn}$ will be unknown and hence, will be estimated using the product moment correlation of normal quantiles corresponding to the observed scores from the K modalities. We denote the density of C_R^K by

$$C_R^K(u_1, u_2, ..., u_k) \equiv \frac{\partial C_R^K(u_1, u_2, ..., u_k)}{\partial u_1 \partial u_2 ... \partial u_K}$$

$$= \frac{\phi_R^K(\Phi^{-1}(u_1), \Phi^{-1}(u_2), ..., \Phi^{-1}(u_K))}{\prod_{k=1}^K \phi(\Phi^{-1}(u_k))} \quad (7)$$

where $\Phi_R^K(x_1, x_2, ..., x_K)$ is the joint probability density function of the K-variate normal distribution with mean 0 and covariance matrix R, and $\phi(x)$ is the standard normal density function. We will assume that the joint distribution function of genuine (impostor) matching scores for K modalities, $F_{gen}^K(F_{imp}^K)$, is of the form (5) for some correlation matrix R_0 *(R1)*. For the genuine (impostor) case, H_k will be estimated by $L_{gen,k}(x)$ $(L_{imp,k}(x))$ for $k = 1, 2, ..., K$.

3 Fusion Based On Generalized Densities

Two methods of fusion have been considered in this paper. The first method assumes independence between the K biometric modalities and combines the estimated marginal densities using the product rule. For the matching score set $S = (S_1, S_2, ..., S_K)$, the product fusion score of S, *PFS(S)*, is given by

$$PFS(S) = \prod_{k=1}^{K} \frac{l_{gen,k}(S_k)}{l_{imp,k}(S_k)} \quad (8)$$

where $l_{gen,k}(\cdot)$ and $l_{imp,k}(\cdot)$ are the estimates of generalized densities of the genuine and impostor scores of the k^{th} biometric modality. The copula fusion rule combines the individual modalities using the estimated Gaussian copula functions for the score distributions. The copula fusion score of a matching score set $S = (S_1, S_2, \ldots, S_K)$, $CFS(S)$, is given by

$$CFS(S) = PFS(S)\cdot\frac{C_{R_0}^{K}(\Phi^{-1}(L_{gen,1}(S_1)),\Phi^{-1}(L_{gen,2}(S_2)),\ldots,\Phi^{-1}(L_{gen,K}(S_K)))}{C_{R_1}^{K}(\Phi^{-1}(L_{imp,1}(S_1)),\Phi^{-1}(L_{imp,2}(S_2)),\ldots,\Phi^{-1}(L_{imp,K}(S_K)))} \quad (9)$$

where $L_{gen,k}(S_k)$ and $L_{imp,k}(S_k)$ are, respectively, the estimates of generalized distribution functions for the k^{th} biometric modality, and c_R^K is the density of C_R^K as defined in (7). This fusion rule assumes that the Gaussian copula functions can adequately model the dependence between the K biometric modalities.

4 Experimental Results

Experiments on fusion of matching scores using rules (8) and (9) were carried out on two different multimodal databases. For each experiment, 70% of the genuine and impostor matching scores were randomly selected to be the training set for the estimation of the generalized densities and the correlation matrices. The remaining 30% of the genuine and impostor scores were used to generate the ROC curves. This training-testing partition was repeated 20 times and the performance results reported for each value of FAR(False Accept rate) are the median GAR(Genuine Accept Rate) values.

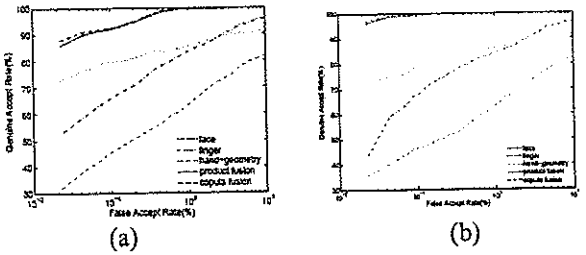
4.1 Databases

The first database which is referred to as the EXP-Multimodal database, consisting of 250 "virtual" subjects each providing five samples of face, fingerprint (left-index) and hand-geometry modalities collected using different sensors and over different time periods. Face images were represented as eigenfaces[15] and the Euclidean distance between the Eigen coefficients of the template-query pair was used as the distance metric. Minutia points were extracted from fingerprint images and the elastic string matching technique [16] was used for computing the similarity between two minutia point patterns. Fourteen features describing the geometry of the hand shape [17] were extracted from the hand images and Euclidean distance was computed for each template-query pair. Experiments were also conducted on the first partition of the Biometric Scores Set - Release I (BSSR1) released by NIST [18].

Table 2 Multimodal Databases

Database	Modalities	K	No.of users
EXP-Multimodal	Fingerprint, Face, Hand-geometry	3	250
NIST-Multimodal	Fingerprint(Two fingers), Face (Two matches)	4	517

The NIST-Multimodal database consists of 517 users and is "truly multimodal" in the sense that the fingerprint and face images used for genuine matching score computation came from the same individual. One fingerprint score was obtained by comparing a pair of impressions of the left index finger and another score was obtained by comparing impressions of the right index finger. Two different face matchers were applied to compute the similarity between frontal face images. Even though the number of subjects in the NIST database is relatively large, there are only two samples per subject.



(a) (b)

Fig 2. Performance of product and copula fusion on the EXP-Multimodal database based on (a) continuous and (b) generalized density estimates.

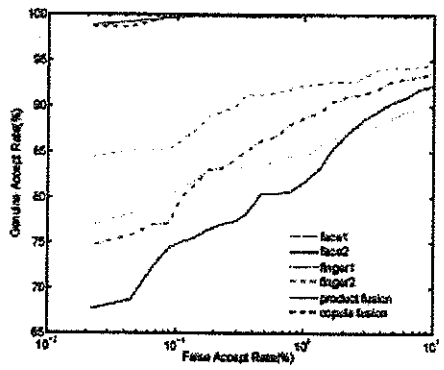


Fig.3. ROC curves for the NIST-Multimodal database for all four modalities

Figure 2 gives the ROC curves for the two fusion rules and the ROC curves based on the matching scores of individual modalities for the EXP-Multimodal database. Figure 2(*a*) shows the recognition performance when the genuine and impostor score distributions of the three modalities are modeled purely by continuous densities. The performance improvement obtained by modeling the matching score distributions as a mixture of discrete and continuous components (generalized densities) can be observed by comparing Figures 2(*a*) and 2(*b*).

The ROC curves for the two fusion rules on NIST-Multimodal database are shown in Figure 3. We can see that both fusion rules give significantly better matching performance compared to the best single modality in each database. It is also observed that the best single modality in both the databases is uncorrelated to the other modalities. For the EXP-Multimodal database, the estimates of the correlation of the best single modality (fingerprint) with the other two modalities (face and hand-geometry) are -0.01 and -0.11 for the genuine scores, and -0.05 and -0.04 for the imposter scores.

5 Conclusion

Based on the generalized density estimates of the genuine and impostor matching scores, two methods of fusion that follow the Neyman-Pearson rule are described. The first fusion rule computes the product of the likelihood ratios for each component modality of a multimodal system and is optimal when the modalities are independent of each other. The second fusion rule assumes that the generalized joint density of matching scores can be modeled using a Gaussian copula function and is a generalization of the product rule when the component modalities are not independent. Experimental results indicate that the two fusion rules achieve better performance compared to the single best modality in both the databases. The proposed method bypasses the need to perform score normalization and choosing optimal combination weights for each modality on a case-by-case basis. In this sense, the proposed solution is a principled and general approach that is optimal when the genuine and impostor matching score distributions are either known or can be estimated with high accuracy.

References

[1] Jain, A.K., Ross, A., Prabhakar, S, *"An Introduction to Biometric Recognition"*, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics 14 PP 4–20, 2004.

[2] Jain, A.K., Ross, A, *"Multibiometric Systems. Comm. of the ACM"*, Special Issue on Multimodal Interfaces 47 PP 34–40, 2004.

[3] Ross, A., Jain, A.K, *"Information Fusion in Biometrics. Pattern Recognition Letters"*, Special Issue on Multimodal Biometrics 24 PP 2115–2125, 2003.

[4] Bigun, E.S., Bigun, J., Duc, B., Fischer, S, *"Expert Conciliation for Multimodal Person Authentication Systems using Bayesian Statistics"*, Proceedings of First International Conference on AVBPA, Crans-Montana, Switzerland PP 291–300, 1997.

[5] Kittler, J., Hatef, M., Duin, R.P., Matas, J.G, *"On Combining Classifiers"*, IEEE Transactions on Pattern Analysis and Machine Intelligence 20 PP 226–239, 1998.

[6] Lam,L., Suen, C.Y, *"Optimal Combination of Pattern Classifiers"*, Pattern Recognition Letters 16 pp 945–954, 1995.

[7] Wang, Y., Tan, T., Jain, A.K, *"Combining Face and Iris Biometrics for Identity Verification"*, Proceedings of Fourth International Conference on AVBPA, Guildford, U.K. PP 805–813, 2003.

[8] Toh, K.A., Jiang, X., Yau, W.Y, *"Exploiting Global and Local Decisions for Multi-modal Biometrics Verification"*, IEEE Transactions on Signal Processing 52 PP 3059–3072, 2004.

[9] Snelick, R., Uludag, U., Mink, A., Indovina, M., Jain, A.K, *"Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems"*, IEEE Transactions on Pattern Analysis and Machine Intelligence 27 PP 450–455, 2005.

[10] Griffin, P, *"Optimal Biometric Fusion for Identity Verification"*, Identix Corporate Research Center Preprint RDNJ-03-0064 (2004)

[11] Prabhakar, S., Jain, A.K, *"Decision-level Fusion in Fingerprint Verification"*, Pattern Recognition 35 PP 861–874, 2002.

[12] Wand, M.P., Jones, M.C.: Kernel *"Smoothing. Chapman & Hall"*, CRC Press (1995)

[13] Nelsen, R.B, *"An Introduction to Copulas"*, Springer (1999)

[14] Cherubini, U., Luciano, E., Vecchiato, W, *"Copula Methods in Finance"*, Wiley (2004)

[15] Turk, M., Pentland, A, *"Eigenfaces for Recognition"*, Journal of Cognitive Neuro-science 3 PP 71–86, 1991.

[16] Jain, A.K., Hong, L., Bolle, R, *"On-line Fingerprint Verification"*, IEEE Transactions on Pattern Analysis and Machine Intelligence 19 PP 302–314, 1997.

[17] Jain, A.K., Ross, A., Pankanti, S, *"A Prototype Hand geometry-based Verification System"*, Proceedings of 2nd International Conference on AVBPA, Washington D.C., USA 166–171

[18] National Institute of Standards and Technology: NIST Biometric Scores Set. Available at http://www.itl.nist.gov/iad/894.03/biometricscores.

Author's Biography

Devireddy Srinivasa Kumar received the B.E. degree in Computer Science & Engineering from Karnataka University, Dharwad in 1992 and M.S. degree in Software Systems from Birla Institute of Technology and Science, Pilani in 1995. He is currently working as a faculty member in the department of Computer Science & Engineering, Nalanda Institute of Engineering & Technology, Guntur. He is a member f IEEE. His research interests are in the areas of Biometrics and Image Processing.