IEEE Transactions on Information Forensics and Security
vol. 5, pp. 92-102, Mar. 2010

A NEW FRAMEWORK FOR ADAPTIVE MULTIMODAL BIOMETRICS MANAGEMENT

Ajay Kumar, Vivek Kanhangad, David Zhang

ABSTRACT

This paper presents a new evolutionary approach for adaptive combination of multiple biometrics to ensure the optimal performance for the desired level of security. The adaptive combination of multiple biometrics is employed to determine the optimal fusion strategy and the corresponding fusion parameters. The score level fusion rules are adapted to ensure the desired system performance using a hybrid particle swarm optimization model. The rigorous experimental results presented in this paper illustrates that the proposed score-level approach can achieve significantly better and stable performance over the decision level approach. There has been very little effort in the literature to investigate the performance of adaptive multimodal fusion algorithm on real biometric data. This paper also presents the performance of the proposed approach from the real biometric samples which further validate the contributions from this paper.

1. INTRODUCTION

The biometrics based controlled access to the protected resources has emerged shown to offer higher security and convenience to the users. The security of the protected resources and information can be further enhanced with the usage of multimodal biometrics. The multimodal biometrics management refers to the process which seeks to manage or coordinate the usage of various biometric modalities in a manner that improves the process of data fusion and perception, synergistically. The design of multimodal biometrics system to ensure the varying requirements of security and traffic flow has invited very little attention in the literature. There has been very little work on the theory, architecture, implementation, or the performance estimation of multimodal biometrics system that can adaptively ensure the varying security requirements. Most of the multi modal biometric systems proposed in the literature use a fixed combination rule and a fixed threshold to achieve the desired performance. The

desired performance is often the minimum Equal Error Rate (EER). These systems offer a fixed level of security and often have to contend with high false rejection rate if the security level is at the highest. The parameters of the combination rule employed are tuned to provide the desired performance for a fixed security level. Therefore the performance of these systems is not adaptive to the varying level of security level requirements. However, there are wide ranging applications where a biometric system with multiple levels of security is desirable. Figure 1 shows the typical Receiver Operating Characteristics (ROC) for a biometric system. The highlighted points on the curve indicate the desired operating points for different applications [30]. There are also times when security levels of a biometric system should be set depending on the perceived threat. Therefore reliable multomodal biometrics management algorithms that are adaptive to the desired level of security and traffic flow are desirable. The design and development of such multimodal biometrics systems that can automatically select the best set of fusion rules, fusion rule parameters, and decision threshold to achieve the best performance (security level) is one of the open problems investigated in this paper. The dynamic selection of number of biometric modalities, based on user preferences, user constraints, image/biometric quality, to reliably achieve the desired level of performance is another related problem open in biometrics research.

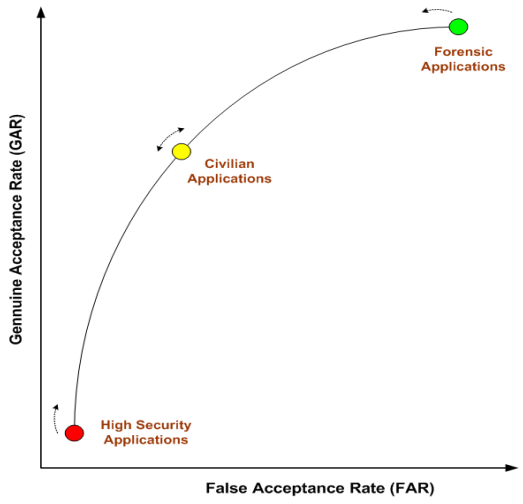


Figure 1: The key operational regions for a typical biometrics system

1.1 Prior Work and Motivation

The biometric systems that employ single biometric trait (unimodal biometric systems) suffer from inherent short comings such as limited discriminability, intra-class variations, vulnerability to spoof attacks, *etc*. The multimodal biometric systems, on the other hand, offer significantly higher security and concomitant reduction in the vulnerability to various attacks. Research efforts on multimodal biometrics have invited lot of attention and several fusion strategies have been proposed in the literature [1]-[4], [12]. Kittler *et al*. [2] have experimented with several fixed combination strategies for performance improvement on real biometrics data. In the context of multi-classifier fusion using score level architecture, it has been shown [3]-[4] that the trainable fusion strategies do not necessarily perform better than fixed combination rules. Authors in [22] proposed an interesting approach to achieve high security using multimodal biometrics. Their approach involves performing continuous verification using user's passively collected fingerprint and face biometric data. However, this approach requires continued physical presence of the user and therefore is not suitable for certain kind of applications including the popular access control applications. Tronci *et al.* [28] have recently investigated another aspect of multimodal problem that focuses on the dynamic selection of matching scores from all the available matching scores. The best matching score from a set of matching scores is selected based on the likelihood of input user being genuine or impostor. However the utility of this approach is quite limited as the achieved performance is not consistent and very little or negligible. BioID system developed by Frischholz *et al.* [23] offers multiple security levels by employing different decision strategies on the biometric modalities (face, lip motion and voice) being fused. When the required security level is low, it may well be enough to make a decision based on the agreement of two out of three modalities. On the other hand, for high security applications, this system demands agreement of all the three modalities. However, BioID system does not provide a systematic way to vary the level of security. Instead, a system administrator makes a decision on the decision

strategies to be adopted to achieve the desired performance.

Veeramachaneni *et al*. [1] have presented a promising approach to the adaptive management of multimodal biometrics to adaptively ensure the desired performance. Authors in [1] employed the decisions from the individual biometric sensors to adaptively select the decision rule that can meet the desired performance constraint. The work detailed in [1], [27] is certainly promising but has several limitations. Firstly, the decision level combination approach has higher performance variations and therefore generates relatively unstable results which require significantly higher number of iterations (average of the results from the hundred runs are employed). In addition, decision level has least information content among other fusion levels (feature level and match score level). Therefore the performance from the combination of abstract labels at the decision level is expected to be quite limited. Matching scores, on the other hand, contain more information than the resulting decisions and therefore adaptive combination of matching scores can lead to better performance. Furthermore, the distribution of matching scores in [1] is assumed to be Gaussian which may not be true for several biometric sensors. The iris is one of the most promising biometric for large scale user identification and its imposter match score distribution has been shown [7] to closely follow the binomial distribution. The Poisson distribution $P_P(m, \lambda)$ of matching score m can be used as convenient approximation to binomial distribution $P_B(m; n, \tau)$ when n is large and τ is small. Another important problem in [1] relates to the usage of only simulated data. There has been no effort to investigate the performance of the adaptive multimodal system performance on real biometric data which makes it very difficult to ascertain its utility.

1.2 Our Work

This work is focused on the development of multimodal biometric system that can include multiple fusion rules in a dynamic architecture to ensure varying security requirements. The main contributions from this paper [32] can be summarized as follows. Firstly, a new approach for the management of access control to ensure the desired level of security (performance) using the adaptive combination of multimodal matching scores is developed. The performance of the proposed approach is ascertained to be superior as compared to the decision-level approach. Secondly, we present the experimental results from the biometric sensors that can generate non-Gaussian distribution of matching scores. Our experimental results show that the proposed score-level approach generates fairly stable performance and requires smaller number of iterations as compared to the decision-level approach employed in [1]. Lastly, but most importantly, this paper shows the utility of adaptive multimodal biometric fusion on the real biometric samples. We also investigate the adaptive combination of iris and palmprint biometric, on publicly available database, to ascertain the average error while achieving/ensuring varying level of security. The results from the real biometric scores also suggest the superiority of score-level ap

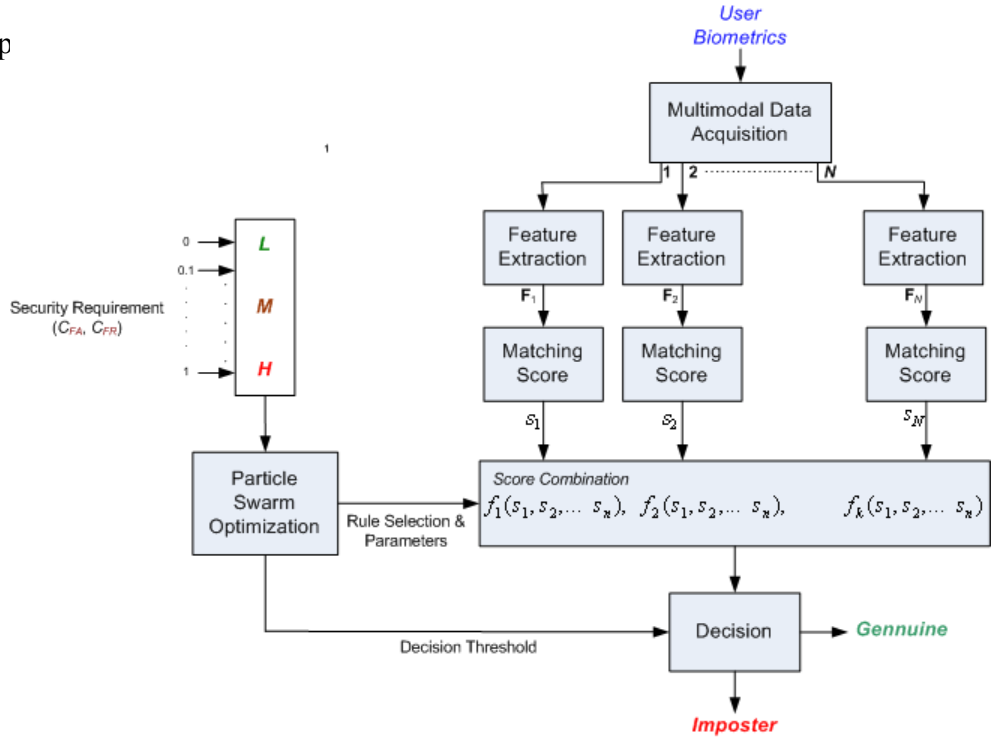


Figure 2: The block diagram of the proposed system using adaptive score-level combination

2. ADAPTIVE MANAGMENT OF SCORES

This paper presents a new framework for the adaptive combination of multimodal biometric sensors. The block-diagram of the proposed approach is shown in figure 2. The multimodal biometric data from N sensors is used to extract the corresponding F_1, F_2, …., F_N feature vectors. These feature vectors are employed to generate the matching scores s_1, s_2, …, s_n from the corresponding templates acquired during the registration.

The management of the multimodal sensors has to be adaptive to the desired level of security. The required level of security is the external parameter that is supplied to the system (figure 2). The *homeland security advisory* [5] system represents a typical example of the qualitative assessment of the adaptive security requirement. Depending on the perceived threat or risk of attack, this system recommends citizens a set of appropriate actions. In a similar way, the risk of attack on a biometric system can be varying and therefore it is critical for it to provide multiple levels of security. The security requirement, in Bayesian sense, is quantified with two parameters; the global cost (0 to 1) of falsely accepting an imposter C_{FA} and the global cost (0 to 1) of falsely rejecting accepting a genuine user C_{FR} from the installed biometrics system. These two costs can be employed to adequately quantify the desired performance. The Bayesian cost E to be minimized by the multimodal biometrics system is the weighted sum of F_{AR} and F_{RR}:

$$E = C_{FA} F_{AR}(\eta) + C_{FR}\, F_{RR}(\eta), \quad \text{where} \quad C_{FA} + C_{FR} = 2 \tag{1}$$

where $F_{AR}(\eta)$ is the global or the combined false acceptance rate and $F_{RR}(\eta)$ is the combined false rejection rate at decision threshold η from the multimodal biometric system. The task of the multimodal biometrics management system (figure 1) is to minimize the (global) cost E, equation 1, by selecting (i) the appropriate score level combination rule, (ii) its parameters and (iii) the decision threshold. The multidimensional search among the various combination rules and their weight

parameters, to optimize the global cost E, is achieved by the particle swarm optimization (PSO) approach.

2.1 Particle Swarm Optimization

Particle swarm optimization is an evolutionary search algorithm developed based on the social behavior of a flock of birds trying to fly to a favorable environment. The PSO [24] is employed to find the solution for the adaptive selection of combination of individual points which are referred as the particles in multidimensional search space. Each particle (representing a bird the flock), characterized by its position and velocity, represents the possible solution in search space. Behavior of the particles in the PSO imitates the way in which birds communicate with each other, while flying. During this communication, each bird reviews its new position in the space with respect to the best position it has covered so far. The birds in the flock also identify the bird that has reached the best position/environment. Upon knowing this information, others in the flock update their velocity (that depends on a bird's local best position as well as the position of the best bird in the flock) and fly towards the best bird. The process of regular communication and updating the velocity repeats until the flock finds a favorable position. In a similar manner, the particle in the PSO moves to a new position in multidimensional solution space depending upon the particle's best position (also referred to as local best position) (p_{ak}) and global best position (p_{gk}). The p_{ak} and p_{gk} are updated after each iteration whenever a suitable, *i.e*. lower cost, solution is located by the particle. The velocity vector of each particle represents/determines the forthcoming motion details. The velocity update equation [6] of particle a of the PSO, for instance (t +1), can be represented as follows:

$$v_{ak}(t+1) = \omega v_{ak}(t) + c_1 r_1 \left(\rho_{ak}(t) - x_{ak}(t)\right) + c_2 r_2 \left(\rho_{gk}(t) - x_{ak}(t)\right) \tag{2}$$

where ω is the inertia weight between 0-1 and provide a balance between global and local search abilities of the algorithm. The accelerator coefficients c_1 and c_2 are positive constants, and r_1 and r_2 are two random numbers in 0-1 range. The corresponding position vector is updated by

$$x_{ak}(t+1) = x_{ak}(t) + v_{ak}(t+1) \tag{3}$$

The equation (2) indicates that the new velocity of a particle in each of its dimensions is dependent on the previous velocity and the distances from previously observed best solutions (positions of the particle).

The particle swarm optimization approach detailed above operates on continuous space. However, there exists optimization problems where the particles are better represented as discrete binary variables. Such problems require that these binary particles be evolved to obtain an optimal solution. A binary version of the particle swarm optimization algorithm is also described in reference [24]. The position vector for each particle in binary PSO can have a value of either zero or one on each dimension. The formula for calculating the velocity update in binary PSO remains the same as real valued version, except that ρ_{ak}, x_{ak} and ρ_{gk} in equation (2) are binary valued. The velocity v_{ak} for binary PSO represents the probability of bit x_{ak} taking the value 1. A sigmoid function *S* is employed to limit the value of the probability v_{ak} to the range [0, 1]. Therefore the position vector of a particle in binary PSO is updated as follows:

$$x_{ak}(t+1) = \begin{cases} 1 & \text{for } r_3 < S(v_{ak}(t+1)) \\ 0 & \text{Otherwise} \end{cases} \tag{4}$$

where $S(v_{ak}(t+1)) = \dfrac{1}{1+\exp(-v_{ak}(t+1))}$ and r_3 is a random number in the interval [0, 1] with uniform distribution.

2.2 Score-Level Combination

The block diagram in figure 2 shows the framework for combining match scores from multiple biometric traits. In this work, we considered four score level combinations from sum or average, product, exponential sum and tan-hyperbolic sum. In fact any number of score level combination rules can be incorporated by expanding the proposed framework. The combined matching score S from each of these combinations is obtained as follows:

$$\text{Sum} \quad - \quad S = \sum_{j=1}^{n} s_j w_j \,, \tag{5}$$

$$\text{Product} \quad - \quad S = \prod_{j=1}^{n} s_j^{w_j} \tag{6}$$

$$\text{Exponential Sum} \quad - \quad S = \sum_{j=1}^{n} \exp(s_j) w_j \tag{7}$$

$$\text{Tan-hyperbolic Sum} \quad - \quad S = \sum_{j=1}^{n} \tanh(s_j) w_j \tag{8}$$

The PSO is employed to dynamically select the appropriate decision threshold and the weights (w_j) to minimize the fitness function, *i.e*., Bayesian cost in equation (1), from each of the possible score-level combinations. In our implementation, each particle is characterized by three continuous variables; the parameters of score level fusion rule w_1 and w_2, decision threshold *thr* and a two bit discrete binary variable representing four different score level fusion rules. Therefore we employ a hybrid PSO with real valued and binary versions of the algorithm to determine the optimal fusion strategy and the corresponding fusion parameters.

3. EXPERIMENTS AND RESULTS

The effectiveness of the proposed scheme is ascertained from the rigorous experiments on the real biometric samples and also from the random samples generated from the real biometric matching

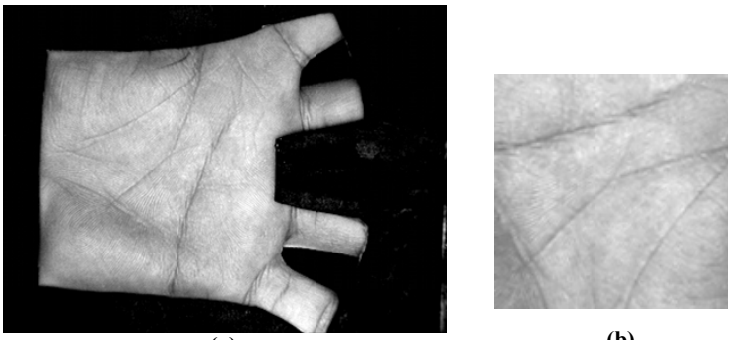
score distributions reported in the literature. The biometric literature is full of examples [31] to suggest that different biometric modalities/databases generate different performances from non-adaptive multi-biometrics system. In order to (i) estimate more reliable estimate on the performance and (ii) achieve better generalization of performance from the proposed framework, the experimental results from various publicly available biometric databases is reported in this paper. We firstly present the experimental results from the real biometric samples which include the combinations from (i) iris and palmprint, (ii) face and speech, and (iii) fingerprint and hand geometry in section 3.1, 3.2, and 3.3 respectively. This is followed by the experimental results from the random samples generated from the (i) Beta-Binomial, (ii) Poisson and (iii) Gaussian distributions.

3.1 Iris and Palmprint

The iris has emerged as one of the most promising modality for the large scale user identification and highly suitable candidate for any multimodal biometric system. The literature on palmprint identification [13]-[15] has suggested reliable performance on the large databases. We therefore firstly investigated the performance of the proposed scheme on the adaptive combination of iris and palmprint biometrics. The database employed for the performance evaluation is publicly available on [16] and [18] respectively. The IITD iris database [18] consists of low resolution 320 × 240 pixel iris images from the 224 users. Therefore the first 224 palmprints from the PolyU palmprint database were randomly paired and employed for the experiments. The iris image normalization, enhancement, feature extraction, were same as detailed in [17]. The figure 3 shows a sample of iris image along with the enhanced normalized image from our database. The combination of log-Gabor and Haar wavelet filters, as detailed in [17], was used to extract the features from each of the 48 × 432 pixels normalized iris images. The steps of image normalization and feature extraction for the palmprint images were similar as detailed in [15]. Figure 4 shows a sample of palmprint image and the corresponding

(a) **(b)**

Figure 3: Image sample from the employed iris images and corresponding normalized enhanced image



(a) **(b)**

Figure 4: Image sample from the employed palmprint images and corresponding normalized enhanced image

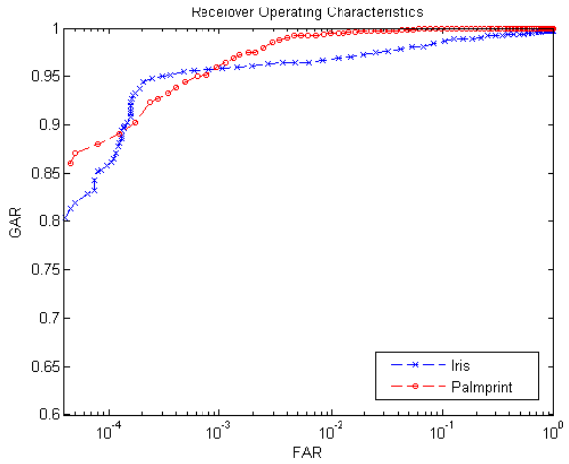
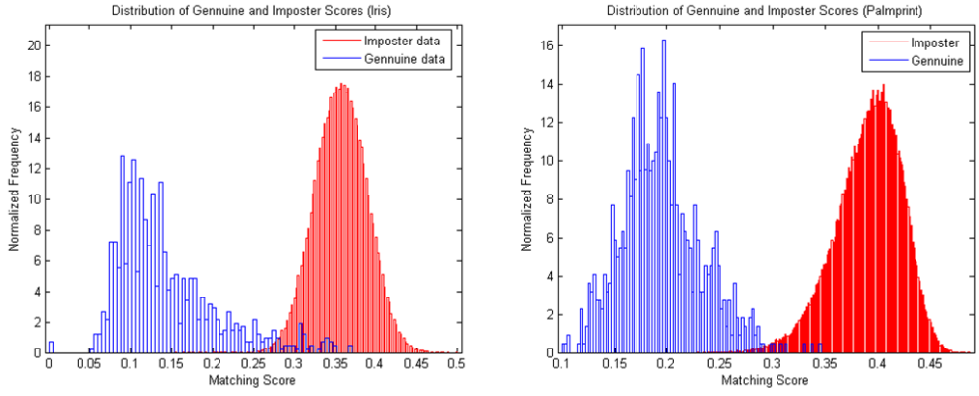


Figure 5: Receiver operating characteristics from the Iris and Palmprint matching scores.



(a) **(b)**

Figure 6: Distribution of matching scores from the two modalities; (a) Iris and (b) Palmprint

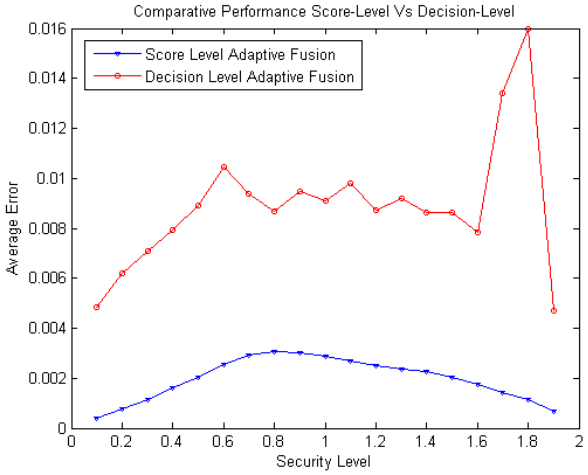


Figure 7: Average minimum error from the score level and decision level approach using the adaptive combination of iris and palmprint modalities

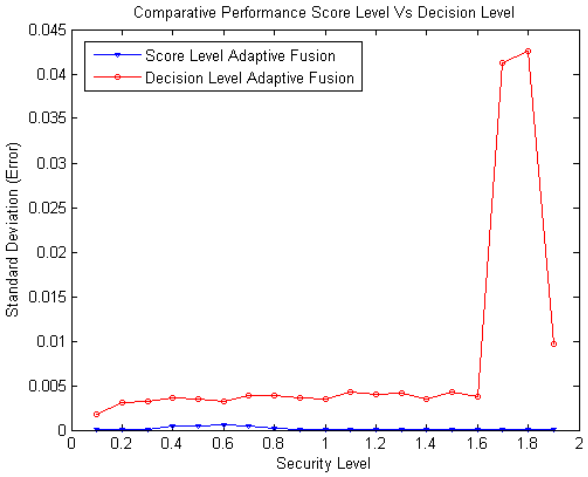


Figure 8: Standard deviation of the minimum error, from each run, using score level and decision level approaches

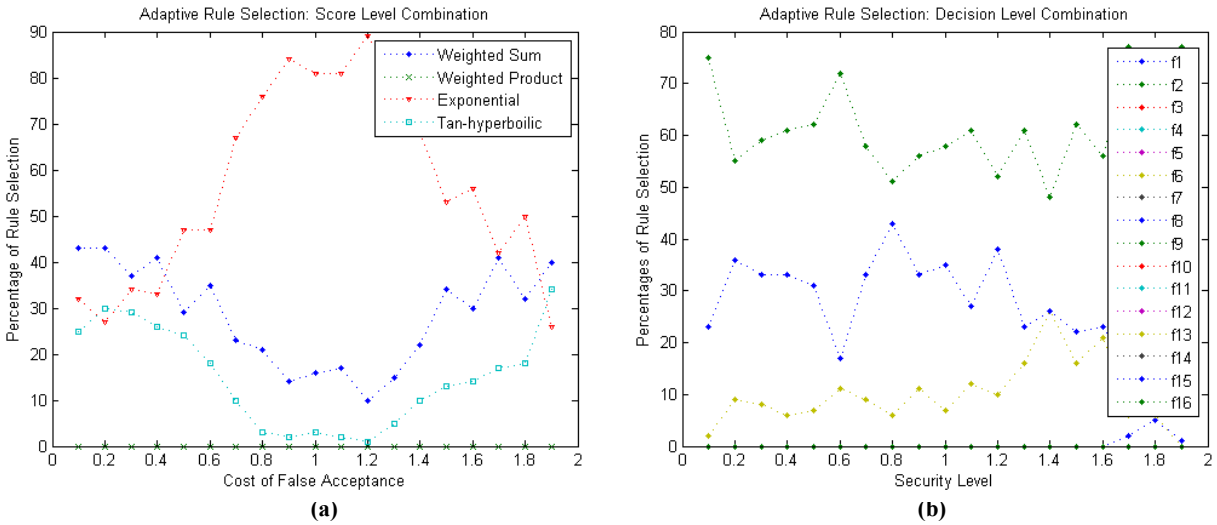


Figure 9: Adaptive selection of fusion rules using score level combination (a) and decision level combination (b)

normalized region of interest employed for the feature extraction. We employed 35 × 35 ordinal mask with $\delta_x = 3$, $\delta_y = 10$ to extract ordinal features from every 128 × 128 pixel normalized palmprint image. The PSO parameters c_1, c_2, ω were experimentally selected and fixed at 1, 1, 0.8 respectively for all the experiments reported in this paper. The initial positions of the particle are randomly selected in the search space (uniform distribution assumption). Therefore the PSO generates varying results from each run and the experimental results from the average of the results in several runs are employed.

The receiver operating characteristics from the iris and palmprint are shown in figure 5, while the distribution of genuine and imposter matching scores is shown in figure 6. Figure 7 shows the average of the minimum *weighted error rate*, achieved from the proposed score level adaptive combination scheme, for varying security requirements. This *security level* is essentially the sum of cost of false acceptance (C_{FA}) and cost of false rejection (C_{FR}). Therefore whenever the security level is varied in the *x*-axis of figure 7, we actually traverse from one end of the receiver operating characteristics to other end (figure 1). This figure also illustrates the average of minimum error when the decision-level approach is employed. It can be observed from this figure that the average error rate is always minimum, for all the selected costs or security level, using proposed score-level scheme as compared with the error rate obtained from the decision-level approach in [1] [27]. While incorporating the decision-level approach, we report the results from 100 runs as used in [1]. The figure 8 shows the standard deviation of the minimum error, from each run, for the decision level approach and those from the score-level approach. It can be observed that the results from the proposed scheme are significantly stable, *i.e.*, have smaller (near zero) standard deviation, and therefore require significantly smaller number of iterations. Our observations have suggested (figure 8) that only single run is adequate to achieve the stable results from score-level combination as compared to the 100 runs employed for decision-level approach. The figure 9(a) and 9(b) shows the adaptive

selection of score level and the decision level rules respectively, with the variation of security level, obtained from this set of experiments.

3.2 Face and Speech

Another set of experiments was performed on the synchronized face and speech database from 295 subjects using the publicly available XM2VTS [20] database. This database is divided into set of 200 gennuine and 70 imposter subjects while the rest of 25 subjects are employed for evaluation imposters using Lausane Protocol (LP1) as detailed in [21]. The DCT (Discrete Cosine Transform) coefficients from each of the 80 × 64 pixel face images are used to generate matching scores using GMM (Gaussian Mixture Model). The LFCC (Linear Filter-Bank Cepstral Coefficient) obtained from the speech data in 20 milliseconds window is used to generate genuine and imposter matching scores using GMM. The extraction of features and corresponding matching scores is detailed in reference [21]. The ROC from the test samples for face and speech biometric is shown in figure 10 while the distribution of genuine and imposter matching scores is shown in figure 11(a)-(b). It can be observed from figure 11(c) that the weighted sum, tan-hyperbolic sum, and weighted product combination is adaptively selected as the security level in varied in the range 0-2. The summary of experimental results presented in figure 11 from XM2VTS database again confirms the advantage of proposed adaptive score-level approach

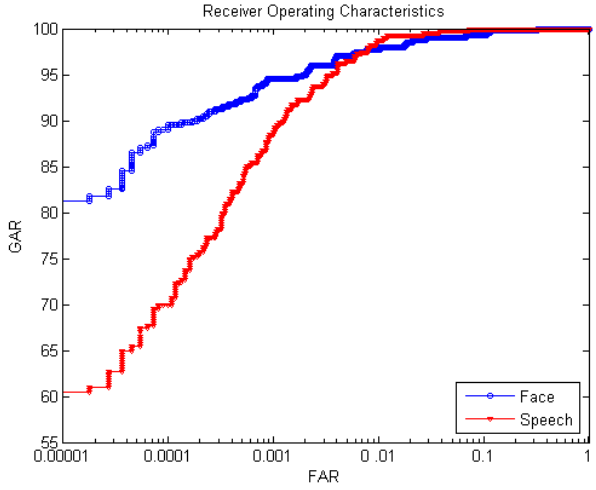


Figure 10: Receiver operating characteristics for face and speech biometric samples using XM2VTS database.

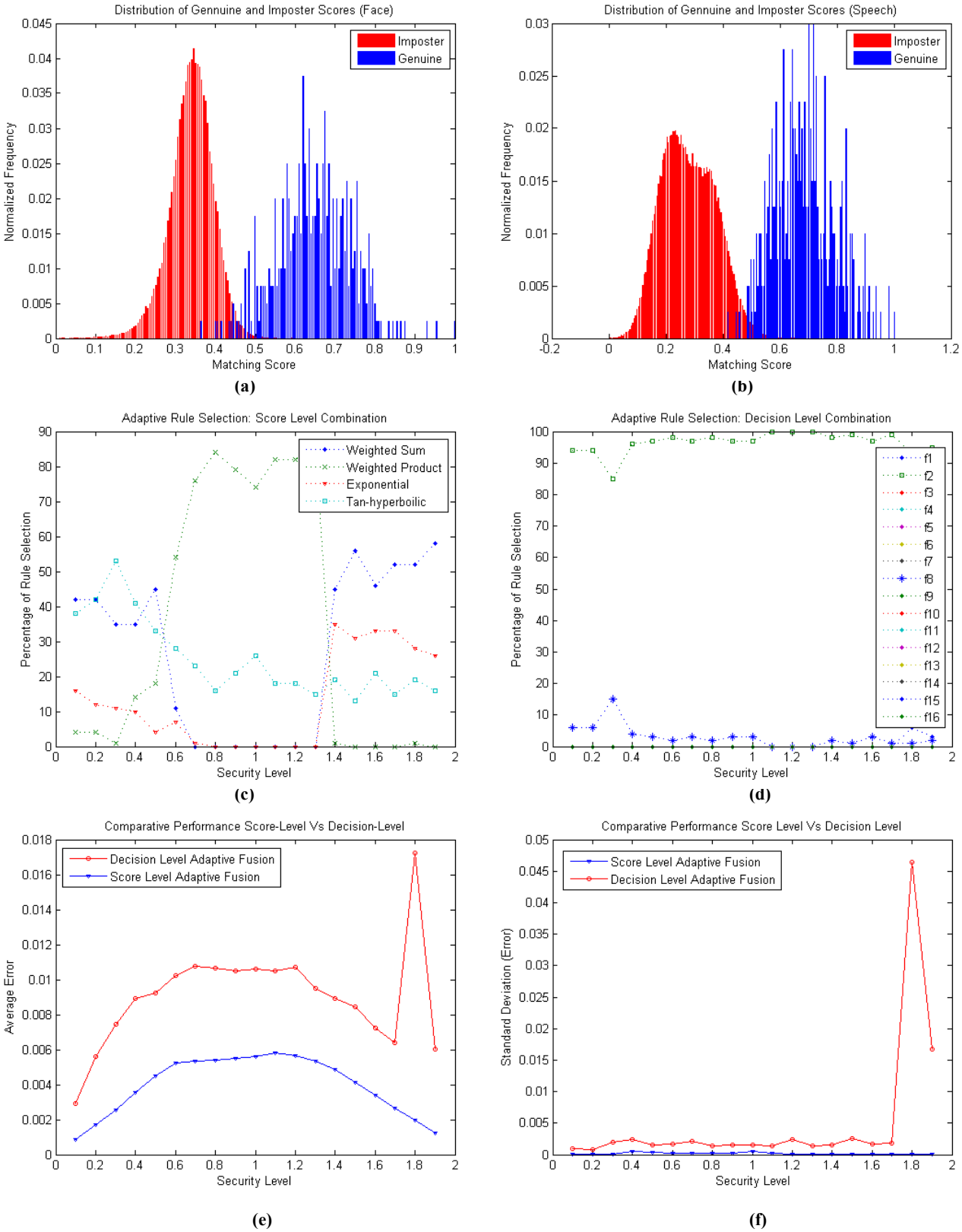


Figure 11: Distribution of matching scores from face and speech biometric samples in (a) and (b) respectively; adaptive selection of fusion rules using score level and decision level in (c) and (d) respectively; the average and standard deviation of minimum error from the adaptive score and decision level combination in (e) and (f) respectively

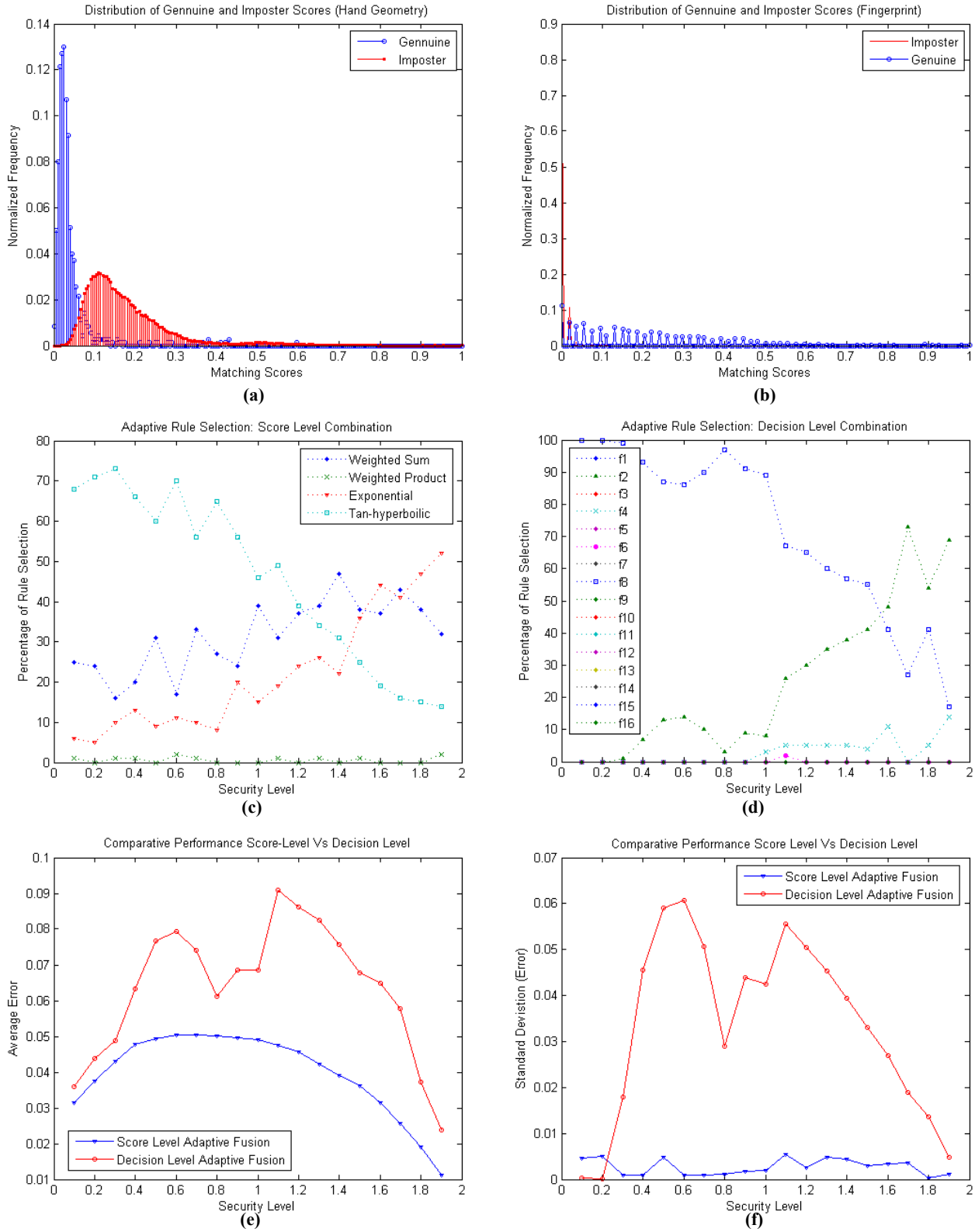


Figure 12: Distribution of matching scores from hand geometry and fingerprint biometric in (a) and (b) respectively; adaptive selection of fusion rules using score level and decision level in (c) and (d) respectively; the average and standard deviation of minimum error from the adaptive score and decision level combination in (e) and (f) respectively

3.3 Fingerprint and Hand Geometry

In order to evaluate the performance on real hand biometrics samples, the fingerprint and hand geometry matching scores from the 100 users were employed. The fingerprint images from the FVC2004 DB2 database [10] which are composed of 8 images from each of 100 users were employed. The hand geometry image samples from 100 users, as acquired in [8], were used for the feature extraction. The matching score from these two biometric was generated as detailed in [9], [11]. The 700 gennuine and 69300 imposter scores from each of the two biometric were generated. The fingerprint matching score employed min-max normalization. The distribution of the normalized matching scores from the two biometric modalities is shown in figure [9]. The distribution of fingerprint matching scores is similar to as in [12] mainly due to the usage of FVC2004 DB2 database. The performance from the adaptive combination of hand geometry and fingerprint biometric is shown in figure 12(e)-(f) while the adaptive selection of rules is shown in figure 12(c)-(d). It can be observed from the figure 11 that the performance from the score level adaptive combination is significantly better as compared to the decision level combination.

3.4 Simulated Score Distributions

In this set of experiments, the class conditional matching scores were obtained from the random samples corresponding to the parametric model of given biometrics. The experimental results from the real finger-vein image samples from right index fingers of 506 subjects, as detailed in [25]-[26], are employed to generate the parameters for the genuine and imposter score distributions. The genuine matching score distributions from these 1012 (506 × 2) pairs of identical right index fingers follow the beta-binomial distribution with $n = 400$, $\alpha = 8.49$, and $\beta = 94.19$.

$$P_{BB}(s_i|n_i,\alpha,\beta) = \binom{n_i}{s_i} \frac{B(\alpha+s_i,\beta+n_i-s_i)}{B(\alpha,\beta)} \tag{9}$$

where $B(\alpha, \beta)$ is the complete beta function and (α, β) are its shape parameters [29].

The imposter distributions from 255,530 of matching scores follow normal distribution as detailed in [25]. Therefore 1012 randomly sampled genuine scores corresponding to beta-binomial distribution (m = 400, α = 8.49, and β = 94.19), and 255,530 randomly sampled imposter scores corresponding to normal distributions were employed to ascertain the performance from the adaptive combination of finger-vein biometric from two fingers. The figure 13 (a)-(b) illustrates distribution of genuine and imposter matching scores from the two fingers. The adaptive selection of rules with the varying level of security is illustrated in figure 13(c)-(d) while the comparative performance from the adaptive combination of two finger-vein biometric is illustrated in figure 13(e)-(f). The experimental results in this figure again confirm the significant performance improvement from the proposed score-level adaptive combination scheme as compared to the decision level combination.

The generalization and characterization of genuine and imposter matching scores from the real biometric samples using any specific parametric form is very difficult. Therefore another set of experiments was performed for the case when the score distribution is Poisson. The randomly sampled 1000 genuine and 1,000,00 imposter matching scores, with the mean parameter (λ) 30,40 for first and 38, 48 for the second modality, were employed to ascertain the performance. The experimental results from this set of experiments are summarized in figure 14. These results again confirm the advantages of proposed approach using adaptive score-level combination over decision-level approach when the score distributions are Poisson. It is well-known that the Gaussian distributions does not capture information contained in the tails of distribution while matching score distributions generally have large tail. Therefore Gaussian distribution may not be appropriate to model genuine and imposter score distributions. However, reference [1] presented experimental results from the decision level adaptive combination approach using Gaussian score distributions. Therefore another set of experiments were focused to investigate the performance from unimodal systems whose score

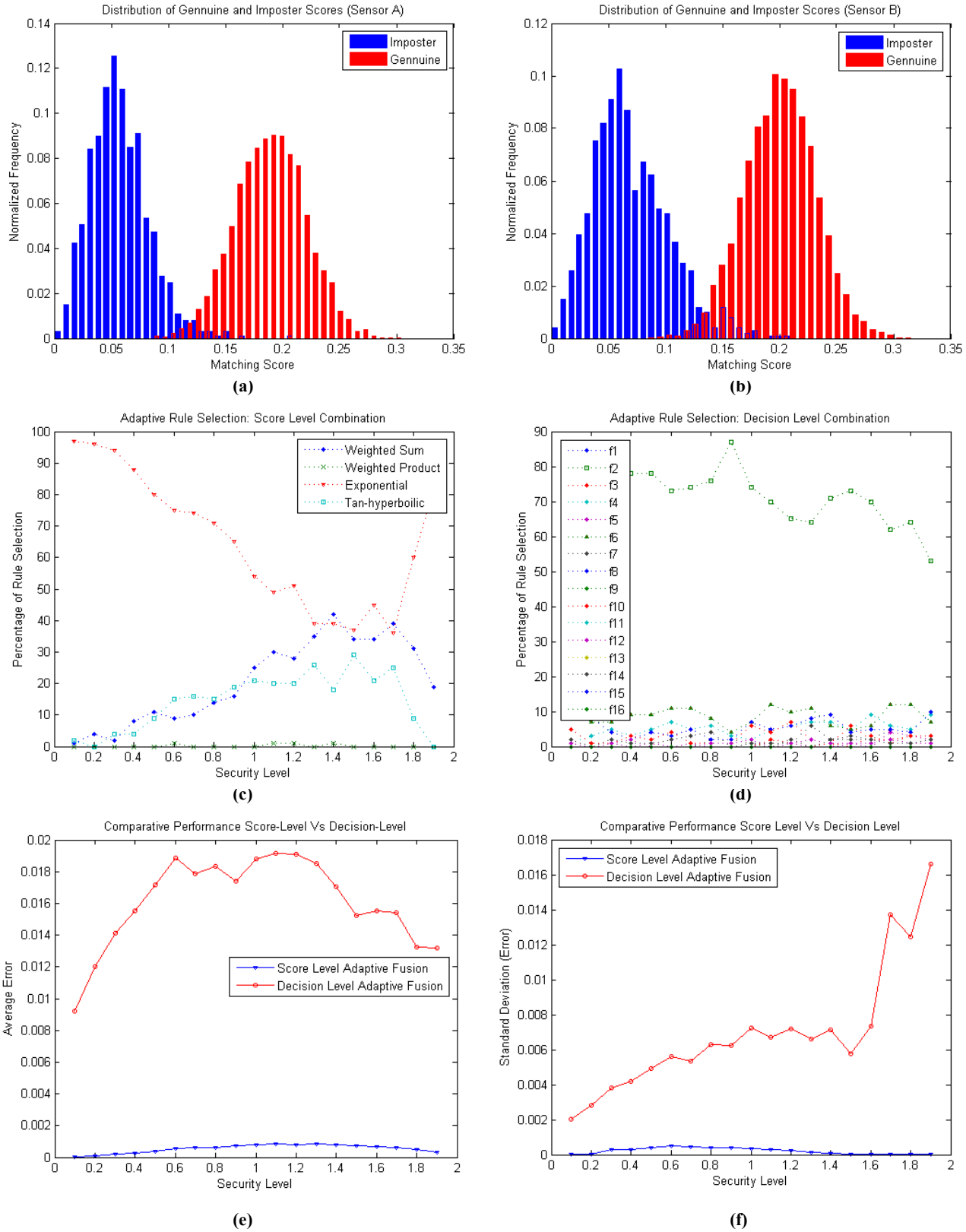


Figure 13: Distribution of matching scores from the beta-binomial distribution for two sensors corresponding to finger vein matching scores in (a) and (b); adaptive selection of fusion rules using score level and decision level in (c) and (d) respectively; the average and standard deviation of minimum error from the adaptive score and decision level combination in (e) and (f) respectively

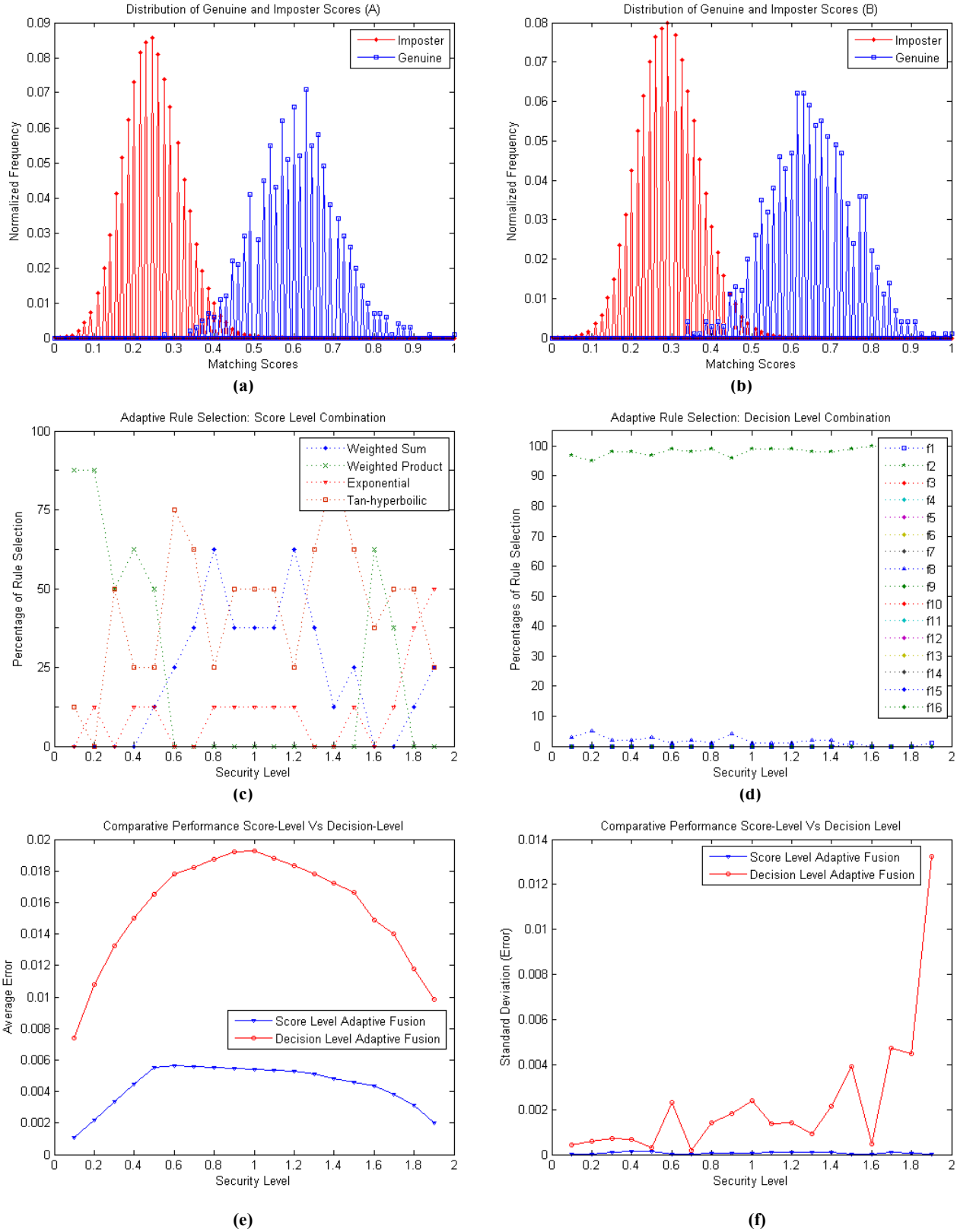


Figure 14: Distribution of matching scores from the two modalities using randomly sampled Poisson distributions in (a) and (b); adaptive selection of fusion rules using score level and decision level in (c) and (d) respectively; the average and standard deviation of minimum error from the adaptive score and decision level combination in (e) and (f) respectively

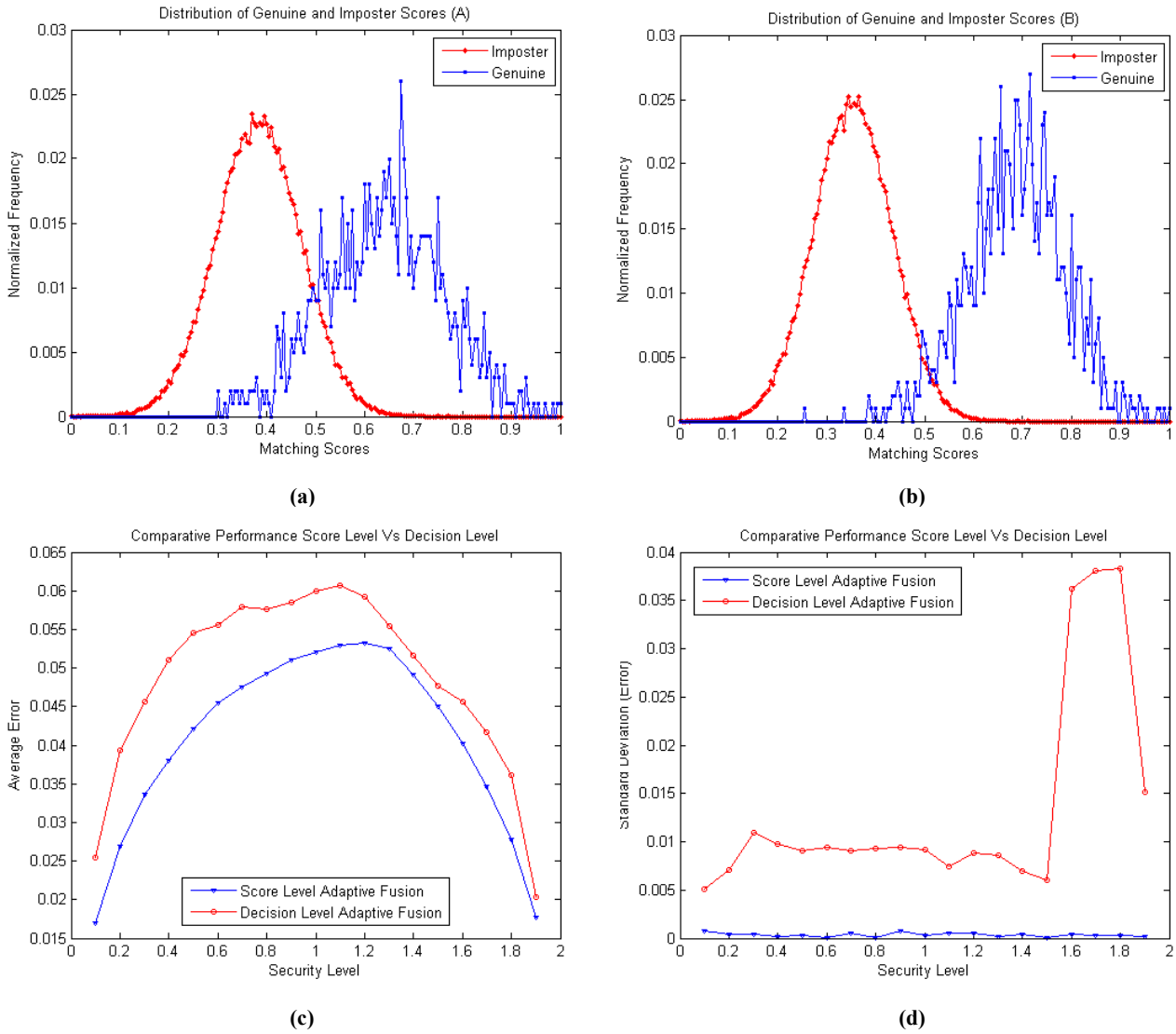


Figure 15: Distribution of matching scores from the two modalities using randomly sampled Gaussian distributions in (a) and (b); the average and standard deviation of minimum error from the adaptive score and decision level combination in (e) and (f) respectively

distribution resemble Gaussian. The distributions of the gennuine matching scores from the two biometric systems, using μ (σ) of 36/12 and 45/10 respectively, was used to ascertain the performance as shown in figure 15. The genuine and imposter distributions from the two biometric modalities in figure 15 consists of 1000 genuine and 1,000,00 imposter scores. The comparative experimental results shown in figure 15 again confirm the advantages of proposed approach using adaptive score-level combination over decision-level approach.

3.5 Discussion

The main objective of our work is to develop a reliable approach for the adaptive combination of multiple biometric modalities to ensure desired level of security. One of the key features of our proposal is the usage of nonlinear score level combination rules in (5)-(8). Our experimentation with the introduction of nonlinearities in equation (6)-(8) has been quite successful. The rigorous experimental results shown in figure 9(a), 11(d), 12(c), 14(c) illustrate the dynamic selection of these nonlinear score level combinations to ensure the desired level of security. The success of this scheme is also attributed to the usage of hybrid PSO, as our goal was not only to ensure appropriate adaptive selection of score level combination but also to select parameters for selected combination.

In multibiometrics, a judiciously designed combination of individual matching scores is expected to yield better performance than combining abstract class labels (decision level approach). The plausible explanation of this superiority lies in the fact that the matching scores can be better exploited to extract higher information content (about the input biometric data and the matching) and are able to provide better representation than the class labels. The disagreement by the individual classifiers in the output of the matching process often deteriorates the performance of a multibiometrics system. However, it is intuitive to think that these conflicting decisions by the matchers can have more adverse effect on the performance in decision level combination than that of score level combination. The experimental results in this paper have also suggested that our proposed framework consistently outperforms the decision level approach, suggested in [1], in terms of standard deviation of error as well. The variation of minimum cost (achieved by the PSO) arises due to the fact that not all the solutions given by the PSO are truly optimal and instead some are suboptimal solutions with a minimum cost very close to the global (true) minimum cost. Since the number of fusion rules in the decision level fusion framework [1] are extremely high (2^{2^N} rules for fusion of N modalities), the

search space for potential optimal solutions becomes very large. This results in increased possibility of PSO converging to sub optimal solutions and thus causing higher standard deviation of minimum cost achieved. Unlike the decision level fusion, number of rules in the proposed fusion framework does not depend on the number of modalities and is quite limited (four rules considered in this work). This explains why the PSO in the proposed framework exhibits significantly less variation in the minimum cost achieved

It is also worth noting that the combination of iris and palmprint biometrics investigated in section 3.1 is new and promising to ensure higher level of security in the proposed framework (figure 2) which has not yet been investigated in the literature. In our experiments, the palmprint features achieved better performance than those from iris images (figure ROC). However, this performance comparison should be interpreted in the context of low resolution and low quality iris images employed from IITD database [18] while palmprint images from PolyU database [16] employed user-pegs which restrict the scale and orientation changes in the acquired images.

4. CONCLUSIONS AND FUTURE WORK

In this paper a new approach for the adaptive combination of multiple biometrics to dynamically ensure the desired level of security is presented. The proposed method uses a hybrid particle swarm optimization to achieve adaptive combination of multiple biometrics from their matching score performance. The rigorous experimental results presented in section 3, from the several public biometric databases (palmprint, iris, face, speech, fingerprint), consistently suggest significant performance improvement from the developed approach. The experimental results also confirms that the proposed score-level approach generates fairly stable performance and requires smaller number of iterations to generate better performance as compared to the decision level approach. It may be noted that the computational complexity of the proposed algorithm for its implementation and deployment

for any real world application is not significant. The hybrid PSO employed in the proposed framework takes up the major share of computational load. However, parameter tuning by the hybrid PSO can be performed offline by computing the optimal parameters (fusion rules, weights and decision threshold) for every possible requirement of input security level in the range 0 to 2 (in steps, say, 0.1) and stored in a look up table. Whenever there is a new requirement for the security level at input, the optimal parameters for that particular security level can be retrieved from the look up table and used for performing authentication/verification tasks. Therefore the verification time from the proposed methodology is quite equivalent to (or comparable with) any other non adaptive multimodal biometric system.

In summary, rigorous experimental results presented in this paper suggest that the dynamic selection of fusion rules and their parameters using the hybrid PSO based approach can offer better performance than the decision level scheme using PSO. There are range of other fixed, non-adaptive, approaches [28], [31], [33] which can also be explored to ascertain if *further* performance improvement can be achieved than those from the adaptive score level combination approach proposed in this paper. The increased complexity resulting from the simultaneous combination of multiple score-level matchers may be justified by either (i) its ability to achieve better performance or (ii) its ability to adaptively move/select the fusion rules and their parameters for the desired level of security. In this work the focus has been on the later, *i.e*. on (ii). Therefore, further work is required to ascertain whether some fixed, non-adaptive, score level combinations for each of the desired/possible level of security can be employed to achieve better performance than the adaptive score level scheme investigated in this paper. Our current efforts are focused to employ significantly larger multimodal database, from the real biometric samples, and generate more reliable estimate on the performance improvement. One of the key problems in adaptive multimodal biometrics management pertains to the

selection of biometric modalities. Therefore future efforts should also be focused to develop algorithms that can adaptively select best set of biometric modalities from the available set to ensure the desired level of security.

5. AKNOWLEDGEMENT

This work was supported in part by a research grant from the Department of Computing, The Hong Kong Polytechnic University (Grant 4-Z0F3) and in part by MCIT, Government of India (Grant 12(54)/2006-ESD).

6. REFERENCES

[1] K. Veeramachaneni, L. A. Osadciw, P. K. Varshney, "An Adaptive Multimodal Biometric Management Algorithm," *IEEE Trans. Sys. Man & Cybern*., *Part-C*, vol. 35, no. 3, pp. 344-356, Aug. 2005.

[2] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, "On combining classifiers," *IEEE Trans. Patt. Anal. Machine Intell.*, vol. 20, pp. 226-239, Mar. 1998.

[3] D. M. J. Tax, M. V. Breukelen, R. P. W. Duin, and J. Kittler, "Combining multiple classifiers by averaging or multiplying," *Pattern Recognition*, vol. 33, pp. 1475-1485, 2000.

[4] F. Roli, S. Raudys, and G. L. Marcialis, "An experimental comparison of fixed and trained fusion rules for crisp classifier outputs," *3rd Intl. Workshop on Multiple Classifier Systems*, MCS 2002, Cagliari (Italy), Springer-Verlag, LNCS, Jun. 2002.

[5] http://www.dhs.gov/xlibrary/assets/CitizenGuidanceHSAS2.pdf

[6] M. Clerc and J. Kennedy, "The Particle Swarm-Explosion, Stability, and Convergence in a Multidimensional Somplex space," *IEEE Trans. Evolutionary Comp.*, vol. 6, p. 58-73, 2002.

[7] J. Daugman, "Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons," *Proc. IEEE,* vol. 94, no. 11, pp 1927-1935, 2006

[8] A. Kumar and D. Zhang, "Hand geometry recognition using entropy-based discretization," *IEEE Trans. Information Forensics & Security*, vol. 2, pp. 181-187, Jun. 2007.

[9] A. Kumar and D. Zhang, "Combining, fingerprint, palmprint and hand-shape for user authentication," *Proc. ICPR*, pp. 549-552, Hong Kong, 2006.

[10] http://bias.csr.unibo.it/fvc2004

[11] T.-Y. Jea and V. Govindaraju, "A minutia-based partial fingerprint recognition system," *Pattern Recognition*, vol. 38, pp. 1672-1684, 2005.

[12] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometricsystems," *Pattern Recognition*, vol. 38, pp. 2270-2285, Dec. 2005.

[13] Z. Sun, T. Tan, Y. Yang, and S. Z. Li, "Ordinal palmprint representation for personal identification," *Proc. CVPR 2005*, pp. 279-284, 2005.

[14] A. K. Jain and M. Demirkus, "On latent palmprint matching," MSU Technical Report, May 2008.

[15] D. Zhang, W. K. Kong, J. You, and M. Wong, "On-line palmprint identification," *IEEE Trans. Patt. Anal. Machine Intell*., vol. 25, pp. 1041-1050, Sep. 2003.

[16] The PolyU Palmprint Database (version 2.0); http://www.comp.polyu.edu.hk/~biometrics

[17] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal identification," *Proc. CVPR 2008*, pp. 21-27, Anchorage, Alaska, Jun 2008.

[18] IITD Iris Database, http://web.iitd.ac.in/~biometrics/Database_Iris.htm

[20] http://www.ee.surrey.ac.uk/CVSSP/xm2vtsdb

[21] N. Poh and S. Bengio, "Database, protocol and tools for evaluating score-level fusion algorithms in biometric authentication," *Research Report IDIAP-RR-04-44*, IDIAP, Switzerland, Aug. 2004. (*With due acknowledgement to Dr. N. Poh, University of Surrey*)

[22] T. Sim, S. Zhang, R. Janakiraman and S. Kumar, "Continuous verification using multimodal biometrics," *IEEE Trans. Patt. Anal. Machine Intell.*, vol. 29, no. 4, pp. 687-700, Apr. 2007.

[23] R. W. Frischholz and U. Deickmann, "BioID: A multimodal biometric identification system," *IEEE Comput.,* vol. 33, no. 2, Feb. 2000.

[24] R. C. Eberhart and J. Kennedy, *Swarm intelligence*, Morgan Kaufmann, San Diego, 2001.

[25] T. Yanagawa, S. Aoki, and T. Ohyama, "Human finger vein images are diverse and its patterns are useful for personal identification", *MHF Technical Report MHF 2007-12*, Kyushu University, 21st Century COE Program, Development of Dynamic Mathematics with High Functionality, Apr. 2007.

[26] H. Ogata and M. Himaga, "Finger vein," *Enclyopedia of Biometrics*, Springer, 2008.

[27] V. Kanhangad, A. Kumar, and D. Zhang, "Comments on 'an adaptive multimodal biometric management algorithm," *IEEE Trans. Sys. Man & Cybern*., *Part-C*, vol. 38, no. 5, pp. 438-440, Nov. 2008.

[28] R. Tronci, G. Giacinto, F. Roli, "Dynamic Score Selection for Fusion of Multiple Biometric Matchers", *Proc. 14th IEEE International Conference on Image Analysis and Processing*, ICIAP 2007, Modena, Italy, pp. 15-20, 2007.

[29] E. T. Bradlow, P. J. Everson, "Bayesian inference for the Beta-Binomial distribution via polynomial expansions," *J. Comput. & Graphical Statistics,* vol. 11, no. 1, pp. 200-207, Mar. 2002.

[30] A. K. Jain, A. Ross, and S. Pankanti, "An Introduction to biometric recognition," *IEEE Trans. Circuits & Sys. Video Tech*., vol. 14, no. 1, pp. 4-20, 2004.

[31] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*, Springer, 2006.

[32] A. Kumar, "Dynamic security management in multibiometrics," in *Multibiometrics for Human Identification*, B. Bhanu and V. Govindaraju (*Eds*), Cambridge, U.K.: Cambridge Univ. Press, 2010.

[33] K. Nandakumar, A. Jain, and A. Ross, "Fusion in multibiometric identification systems: what about the missing data?," *Proc. ICB 2009*, Alghero (Italy), *available online*, Jun. 2009.