Dynamic Security Management in Multi-biometrics

Ajay Kumar
Department of Computing
The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong
Email: ajaykr@ieee.org

Abstract: The multi-biometrics systems that combine multiple pieces of biometric evidences can offer ultra-high security and high anti-spoofing capabilities. However, such high level of security in the multi-biometrics system is generally associated with higher user inconvenience, cost and complexity in the combination of multiple evidences. The real life security requirements can vary dynamically with time/day and a multi-biometrics system installed to ensure ultra-high security at one end should be capable of automatically/adaptively adjusting the required security at the other end. The multi-level level colour coded system developed by the department of homeland security represents a typical example of such dynamic security requirements for the physical security and access control. This chapter presents an overview of dynamic multi-biometrics security and details a new score level approach to ensure multi-biometrics security. The experimental results from this approach have consistently suggested that this approach offers low complexity and achieves better performance than decision level approach. The overview of related work presented in this chapter also outlines the range of open problems in dynamic security management which requires further research and development efforts.

1. Introduction

The biometrics-based personal identification systems offer automated or semi-automated solutions to various aspects of security management problems. These systems ensure controlled access to the protected resources and provide higher security and convenience to the users. The security of the protected resources and information can be further enhanced with the usage of multi- biometrics systems. The multi-biometric systems are known to offer enhanced security and anti-spoofing capabilities while achieving higher performance. These systems can utilize multiple biometric modalities, multiple biometric samples, multiple classifiers, multiple features and/or normalization schemes to achieve performance improvement (please refer to chapter x for more details). However, the higher security and reliability offered by multi-biometrics systems often comes with the additional computational requirements and user inconvenience that can include privacy and hygienic concerns. Therefore the deployment of multi-biometrics systems for civilian and commercial applications is often a judicious compromise between these conflicting requirements. The management of multi-biometric systems to adaptively ensure the varying level of security requirements, user convenience and constraints has invited very little attention in the literature. There has been very little work on the theory, architecture, implementation, or the performance estimation of multi-biometrics that dynamically ensure the varying level of security requirements.

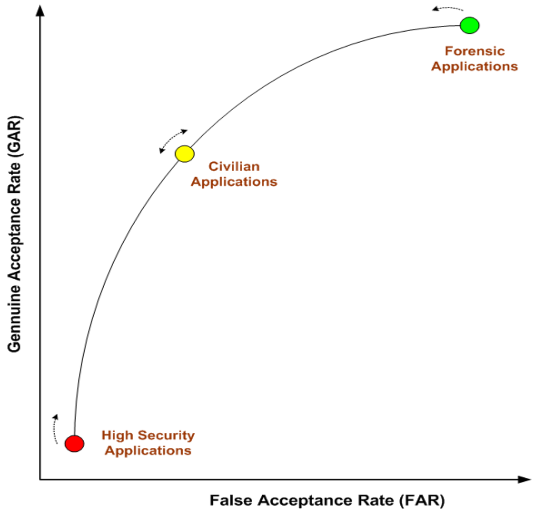


Figure 1: Common operational regions for a typical biometric system.

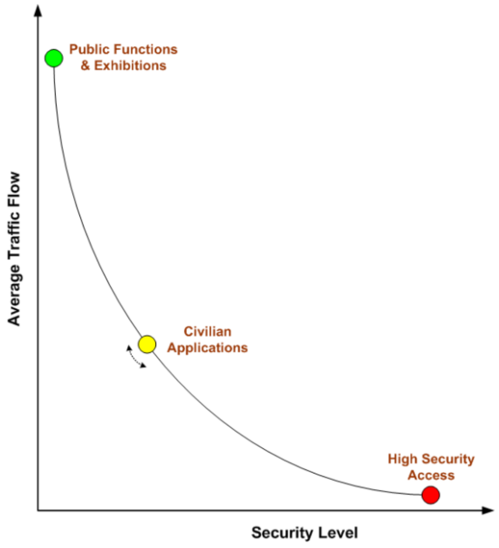


Figure 2: Reduction in average traffic flow with security level.

2. Why Dynamic Security Management?

The expected security requirements from the multi-biometrics systems are typically expressed in terms of error rates and reliability of employed system. These error rates corresponds to false acceptance rate (FAR) which is the rate at which imposters are accepted as genuine users, or false rejection rate (FRR) which is the rate at which genuine users are rejected by the system as imposters.

The reliability of biometric systems largely depends on those controllable factors that directly affect the confidence and stability of decisions (performance measures). These include the ability of multi-biometric system to resist spoof attempts, stability of performance measures with respect to environmental changes such as illumination, humidity and temperature, lifecycle of components, *etc*..

The multi-biometrics systems that employ score level and decision level combinations to consolidate individual scores or decisions are most common in the literature [1], [23]. These systems typically employ a fixed combination rule and a fixed decision threshold to achieve a desired level of performance. The desired level of performance is often the average equal error rate (EER) or the false acceptance rate (FAR). Figure 1 shows a typical Receiver Operating Characteristics (ROC) for multi-biometric system. The highlighted points on this plot show the desired operating points for different applications. It can be observed from this plot that those multi-biometrics system that offer a fixed level of security, say low FAR, have to cope up with associated high false rejection rate (FRR). The higher level of rejection (FRR) by the multi-biometric system for the genuine users causes high inconvenience to the users and also slows average flow of traffic. The average traffic flow refers to the average number of genuine users successfully authenticated by the multi-biometrics system per unit time. Figure 2 illustrates the effect of increasing security level requirement from a multi-biometric system on the average flow of traffic. It can be observed from this figure that the average traffic flow is highest when there is no security requirement and decreases gradually with the increasing requirements of the security. The reduction in average traffic flow could be due to increase in required/average number of attempts from genuine users (due to higher FRR rather than FTE), or due to increase in average time required to authenticate the genuine user resulting mainly from the added complexity of multi-biometric system (added acquisition or processing time). Therefore the conflicting requirements of higher security and average traffic flow require the development of multi-biometric system that can adaptively adjust to the security requirements based of perceived threat. Such systems are expected to automatically adjust the parameters (required number of modalities, fusion parameters, decision threshold, *etc*.) and offer multiple levels of security.

2.1 Objectives

There are potentially large number of applications and scenarios in which different level of security is expected from the same multi-biometric system. Ideally, these systems should be highly flexible to adapt with varying user constraints and expectations. Let us assume that a multi-biometrics system that uses multiple (more than one) modalities for user authentication is deployed to ensure fixed, a minimum, level of security. This system should be designed in such a way that that it is flexible enough to accommodate absence of a particular biometric modality (resulting from poor image/biometric[1] quality or physical challenges) and substitute with another available modality while ensuring the desired (minimum) level of security. This capability requires automated computation and selection of different fusion rules or mechanisms for this substitute modality (s), its parameters, and new decision threshold to ensure desired level of performance. Such systems can also generate adaptive trade off for the poor biometric or image quality by demanding additional biometric samples from the same or different modalities. These systems may also accommodate privacy and hygienic concerns from a user that allows them to refuse a particular (or set) biometric for the authentication. The design and development of such multi-biometric systems that are flexible and can accommodate range of such constraints has large number of civilian and commercial applications.

There are wide ranging applications when the security level of multi-biometrics system should be set depending on perceived threat. The multi-level colour coded citizen advisory system [2] developed by the homeland security department represents a typical example of qualitative assessment of the adaptive security requirement. Depending upon perceived threat or risk of attack,

[1] Poor biometric quality may not be necessarily be due to poor image quality [14].

this system recommends the citizens a set of appropriate actions. These qualitative threat assessments can be employed to set the security level of the deployed multi-biometric system which is capable of adapting to multiple levels of security.

3. Summary of Related Work

The development of multi-biometrics system has invited lot of attention and several fusion strategies have been proposed in the literature [3]-[9], [24]. Kittler *et al*. [3] have experimented with several fixed combination strategies for performance improvement on real biometrics data. In the context of multi-biometrics system, it has been shown [4]-[5] that the trainable fusion strategies do not necessarily perform better than fixed combination rules. Authors in [21] 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. Reference [7] details a multimodal system that offers multiple levels of security by employing different decision strategies for the three biometric modalities (face, lip motion and voice) that can be combined. 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, this 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. Another approach to dynamically achieve higher security is to employ the dynamic selection of matchers as detailed in [8]. The best match score from a set of match scores is selected based on the likelihood of input user being genuine or impostor. The experimental results shown in [8] are quite interesting but require further work as the (i) performance achieved is not consistent as improvement is achieved only for two cases out of four cases considered, and (ii) the performance improvement shown is very little.

An interesting architecture for the dynamic security management involving multiple biometric modalities/sensors and multiple fusion rules has been discussed by Beattie *et al.* [9]. This work envisions a scenario in which a secured building is partitioned into various zones (can be different rooms) and the access rights for each of the users are different for each of these zones. The access decisions in a particular zone may further depend on the outcome of decisions made for access attempts in other zones. In addition, the number of biometric modalities acquired/required in each zone could vary and so is the employed fusion rule. Authors in [9] employ decision level fusion strategies and argued that the moderate level of correlation among different biometric sensors can be safely ignored without any significant impact on accuracy. Another aspect of multi-biometrics security lies in adaptively ensuring the desired performance while automatically responding to user preference, user constraints and aging. The research challenges for such problems are related to the dynamic selection of fusion models, model updating and inference with the models. Reference [20] has suggested semi-supervised learning approach to such adaptive biometrics systems and explores possible research directions.

The adaptive management of multiple modalities/sensors to automatically ensure the desired level of security has been detailed in reference [6]. This approach is certainly promising and probably the first work that employed the decisions from the individual biometric sensors to adaptively select the decision rule that can meet the desired performance/security constraint. The work detailed in [6], [10] provides theoretical framework for the multi-biometrics sensor fusion model and is highly promising but also has some 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. 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 [11] 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 [6] relates to the usage of only simulated data. There has been no effort to investigate the performance of the adaptive multi-biometrics system on real biometric data which makes it very difficult to ascertain its utility. The adaptive score level framework discussed in this chapter attempts to alleviate many of the shortcomings in [6] that employs decision level framework.

4. Quantifying the Security Level

The security of a multi-biometric system can be quantified in terms of the performance indices, *i.e.*, in terms of error rates. The equal error rate (EER) is another commonly employed performance index for biometrics system. However, depending upon applications, the operating point of the multi-biometrics system can be different, *i.e.*, not necessarily EER which is the operating point at which FAR is same as FRR. For high security applications, the cost of accepting imposters as genuine users (FAR) is much higher than the cost (or loss) incurred by rejecting a genuine user as imposters. Therefore, the security level requirements to be achieved (or the expectations) from a multi-biometrics systems, in Bayesian sense, is often quantified using following two parameters;

The global cost of falsely accepting an imposter = $C_{\mathrm{FA}} \in [0,..1]$

The global cost of falsely rejecting a genuine user = $C_{\mathrm{FR}} \in [0,..1]$

The overall or global performance from a multi-biometrics system can be quantified using above two costs. The Bayesian cost E to be minimized by the multimodal biometrics system is the weighted sum of F_{AR} and F_{RR}:

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

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 multi-biometric system. One of the key objectives for the adaptive security management using multi-biometrics system is to minimize the overall (global) cost E, while knowing that the individual FAR and FRR characteristics from the multi-biometrics component sensors are fixed. This can be minimized by selecting (i) the appropriate operating points for the individual multi-biometrics component sensors and (ii) the appropriate combination mechanism rule.

5. Framework for Dynamic Multi-biometrics Management

A generalized framework that can adaptively combine multiple biometric modalities in such a way that the desired level of security (which can vary with time and space) is always ensured has range of applications. Figure 3 shows the block-diagram of such generalized system which responds to the changing needs, *i.e.*, system requirements, and accordingly authenticates the users. The multi-biometrics sensor data from N sensors is employed to firstly extract the corresponding F_1, F_2, …., F_N feature vectors. These feature vectors are then utilized to generate respective matching

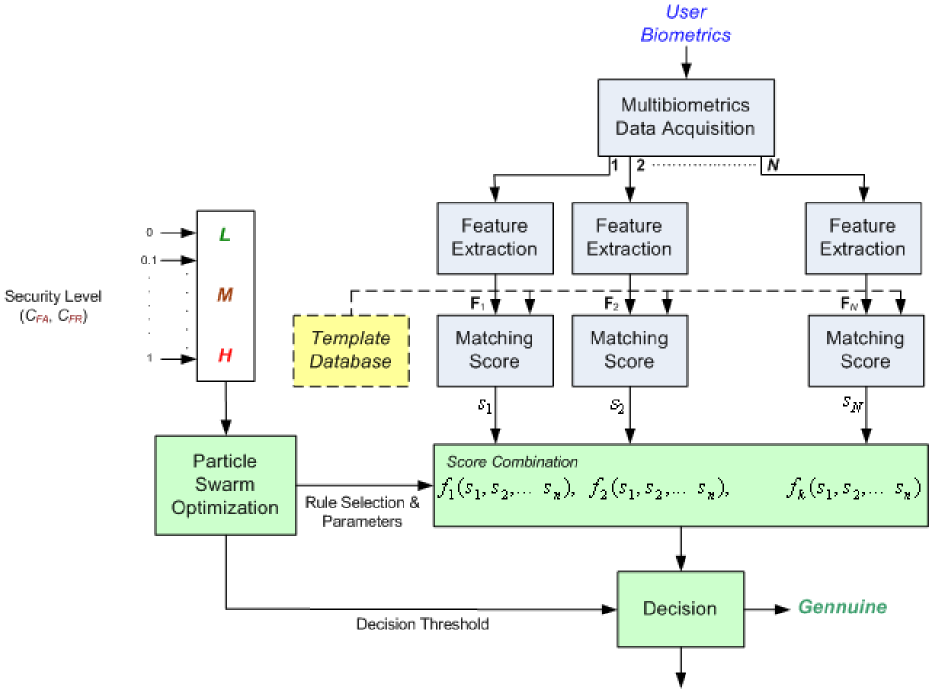


Figure 3: Dynamic security management using adaptive combination of component matching scores.

scores s_1, s_2, …, s_n from the corresponding templates acquired during the registration. The key objective of this system is to select one of the n possible, predefined, score combination rules and a respective decision threshold in such a manner that the security requirements injected into system (from external source) are satisfied. In other word, this multi-biometrics system attempts to minimize the (global) cost E, as illustrated in 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 operating points from individual biometrics and their corresponding combination, to optimize the minimum global cost E, can be achieved by the particle swarm optimization (PSO) approach. Therefore a brief introduction to PSO is provided in section 5.1.

5.1 Particle Swarm Optimization

The PSO 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, characterized by its position and velocity, represents the possible solution in search space. The particle moves to a new position in multidimensional solution space depending upon the particle's best position (p_{ak}) and global best position (p_{gk}). The p_{ak} and p_{gk} are updated after each iterations whenever a suitable, *i.e.* lower cost, solution is located by the particle. The velocity vector of each particle determines the forthcoming motion details. The velocity update equation [12] of particle a of the PSO, for instance (t +1), can be represented as follows:

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

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

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

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).

5.2 Score Level Combinations

The combination matching scores generated from the multi-biometrics sensors require candidate potential score level combination strategies for the consideration of the optimizer (PSO). These matching scores are expected to be uncorrelated. However, this assumption may not be true in real world multi-biometrics system and some moderate level of correlation between matching scores is expected. Therefore, the combination strategies that are effective for both correlated and uncorrelated matching scores deserve consideration. In general, the candidate score level combination strategies to be evaluated by the optimizer (PSO) can be described as follows:

$$S_g = \beta_g(s_j, w_j) \quad j = 1, 2, .. n, g = 1, 2, \dots K \tag{4}$$

where β_g is some nonlinear or linear function of component matching scores and w_j represents corresponding weights. The experimental results on the score level combination have suggested [4] that the sum rule is expected to perform better when some degree of correlation is expected among the matching scores while product rule is expected to perform better on the assumption of independence among the matchers. In the context of score level framework in figure 3, let us consider four (n = 4) possible score level combinations from sum or average, product, exponential sum and tan-hyperbolic sum. The combined matching score S_g from each of these combinations is obtained as follows:

$$S_1 = \sum_{j=1}^{n} s_j\, w_j,\ S_2 = \prod_{j=1}^{n} s_j^{w_j},\ S_3 = \sum_{j=1}^{n} e^{s_j} w_j,\ S_4 = \sum_{j=1}^{n} \tanh\,(s_j) w_j \tag{5}$$

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 the context of score level framework shown in figure 3, 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. The number of decision combination rules required when decisions, rather than scores in (5)-(8), are combined is very high (2^{2^N}) and depends on number of modalities (N) employed in the decision rule based framework in [6]. This results in large search space for locating possible optimal solutions using PSO and likelihood that PSO could converge to sub optimal (or local) solutions. This is the potential limitation of decision-level based approach to meet dynamically changing security requirements in a multi-biometrics system.

6. Experimental Validation and Discussion

The dynamic security management using score level and the decision level framework can be ascertained from the experimental validation on the real multi-biometrics data. Firstly, the experimental results on the publically available National Institute of Standards and Technology, Biometric Score Set Release 1 (NIST BSSR1) database [13] are presented. This is followed by another set of experimental results on publically available iris and palm database.

6.1 NIST BSSR1 Database

The first partition of NIST BSSR1 database consists of matching scores from 517 subjects. In this evaluation all the matching scores from 517 subjects, corresponding to two different face matchers (referred as C and G), are employed as multi-biometrics matching scores. The experimental evaluations using the score level and decision level approach is presented to demonstrate the effect of varying security level on the selection of fusion strategies and the performance, *i.e.*, error in achieving the expected security level (equation 1). The PSO parameters c_1, c_2, ω are empirically selected and fixed at 1, 1, 0.8 respectively for all the experimental evaluations. 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 100 runs are shown.

The ROC from the two face matchers are shown in figure 4, while the distribution of genuine and imposter matching scores is shown in figure 5 (a)-(b). Figure 5(e) shows the average of the minimum *weighted error rate*, achieved from the score level based 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}). This figure also illustrates the average of minimum error when the decision-level approach [6] is employed. It can be observed from this figure that the average error rate is always at minimum, for all the selected costs or security level, using the score-level framework shown in figure 3 as compared with the error rate obtained from the decision-level approach detailed in [6]. The figure 5 (f) shows the standard deviation of the minimum error, from each run, for the decision level approach and those from the score-level approach. The dynamic security management framework formulated in figure 3 generates more stable solution thn the one that can be achieved by decision level framework. This can be ascertained from figure 5(f) which illustrates the comparative variations in the minimum of the costs achieved from each of the 100 runs. The smaller standard deviation from the score level framework in figure 5 (f) means that the large number of iterations are essentially not required for the score level approach. The experimental observations have suggested that only single run may be adequate to achieve the stable results from score-level combination. The adaptability property required for the dynamic security management is clearly demonstrated from the results in figure 5 (c). For example, when the required security level is increased from 0 to 2, different fusion rules (equation 5) are selected by system.

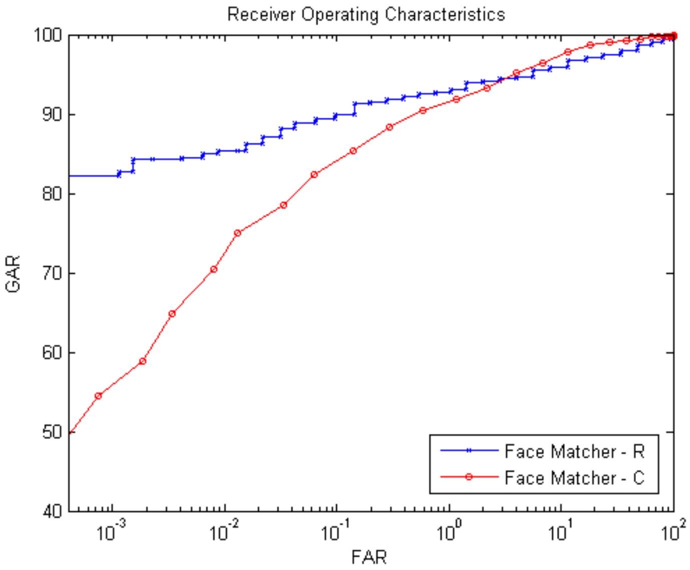
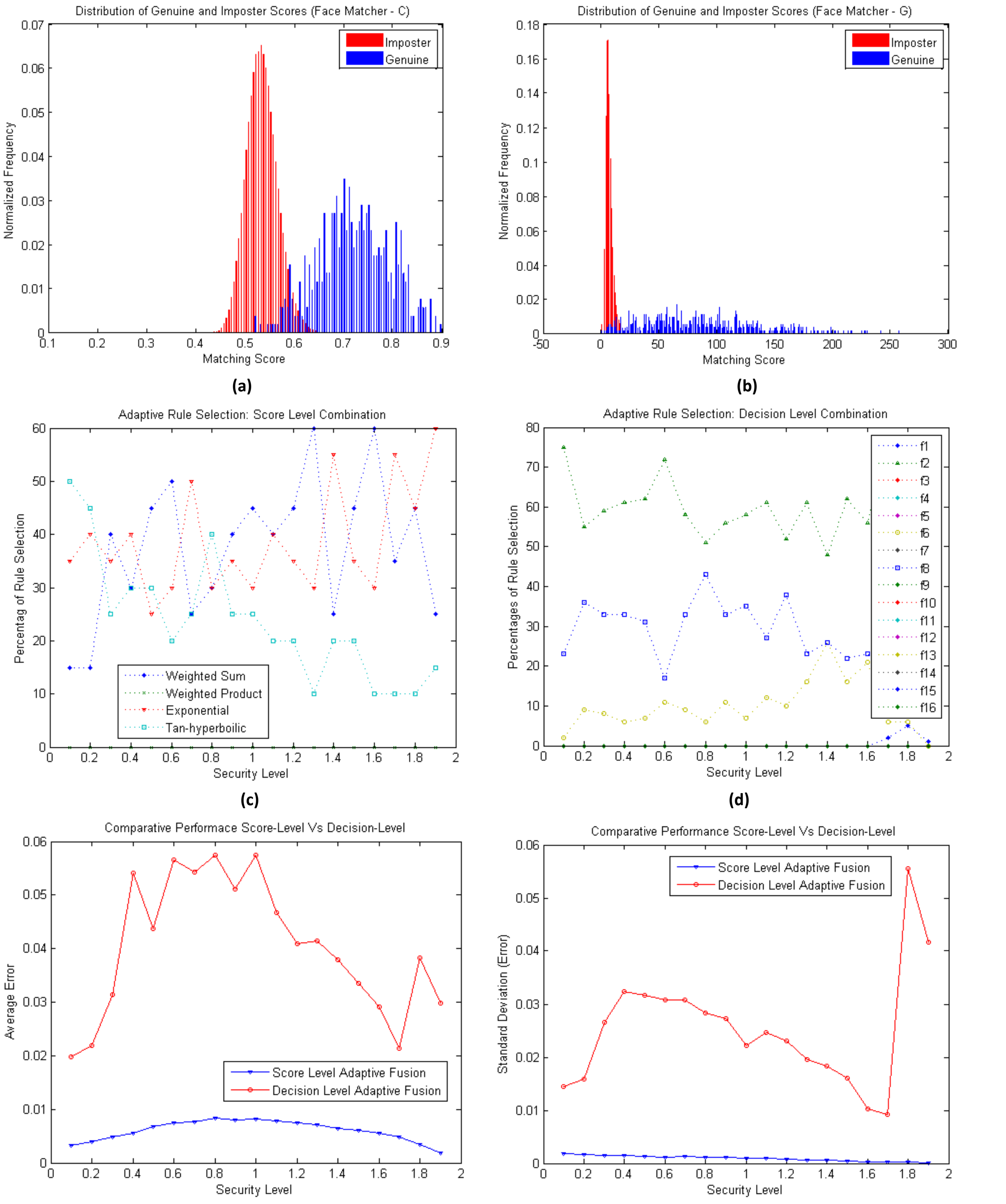


Figure 4: Receiver operating characteristics from two face matchers using NIST BSSR1 database.



(a) **(b)**

(c) **(d)**

(e) **(f)**

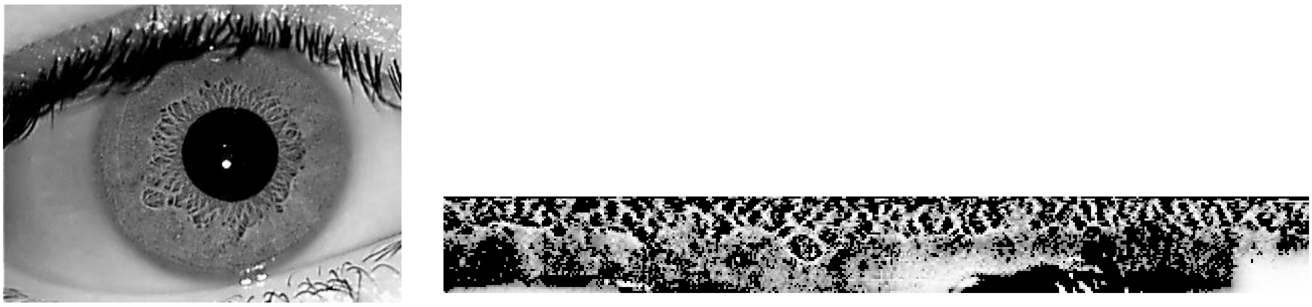
Figure 5: Distribution of matching scores from two face matchers in NIST BSSR1 database in (a) and (b); adaptive selection of fusion rules using score level and decision level in (c) and (d) respectively; the average and standard deviation of minimum error from the adaptive score and decision level combination in (e) and (f) respectively

When the input security level is in the 0-0.2 range tan-hyperbolic fusion rule dominates (appears most number of times), the weighted sum rule appears when the security level is in the range 0.8-1.3 and so on. The corresponding selection of 16 decision level rules [6] is shown in figure 5(d). This explains how the framework for the dynamic management of the security level adaptively selects appropriate combination rules.

6.2 Iris and Palm Database

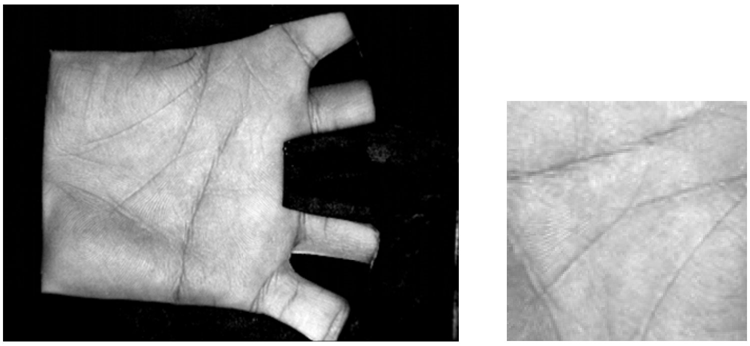
Another set of publically available database employed to demonstrate the effectiveness of the dynamic security management consisted of iris and palmprint images. The iris has emerged as one of the most promising modality for the large scale user identification and highly suitable candidate for any multi-biometrics system. The literature on palm identification [15]-[18] has suggested reliable performance on the large databases. This has been the key motivation in selecting iris and palm modalities for the dynamic security management. The database employed for the performance evaluation is publicly available on [19] and [22] respectively. The IITD iris database [19] consists of low resolution 320 × 240 pixel iris images from the 224 users. Therefore the first 224 palm images from the PolyU palm database were randomly paired and employed in this evaluation. The mutual independence of biometric modalities allows us to randomly augment these biometric modalities that are collected individually. The normalization, enhancement, and feature extraction steps on the iris images are same as detailed in [20]. The figure 6 shows a sample of iris image along with the enhanced normalized image from the IITD database. The combination of log-Gabor and Haar wavelet filters, as detailed in [20], was used to extract the features from each of the 48 × 432 pixels normalized iris images. The steps employed for the segmentation of palm images from the database images were similar as detailed in [17]. Figure 7 shows a sample of palm image and the corresponding normalized region of interest employed for the feature extraction. In this set of experiments, 35 × 35 ordinal mask with $\delta_x = 3$, $\delta_y = 10$ are employed to extract the ordinal features from every 128 × 128 pixel normalized palmprint image. Reference [15] provides further details of the feature extraction and matching criteria employed for the palm images.

The ROC curve corresponding to the iris and palm biometric samples evaluated in this set of experiments is shown in figure 8. The dynamic selection score level and decision level rules are shown in figure 9. This selection is adaptive to the expected level of security desired from the system. The average of the minimum *weighted error rate*, achieved from the score level based adaptive combination scheme, for variation in the expected level of security is shown in figure 10. This figure



(a) **(b)**

Figure 6: Image sample from the employed iris images and corresponding normalized enhanced image



(a) **(b)**

Figure 7: Image sample from the employed palmprint images and corresponding normalized enhanced

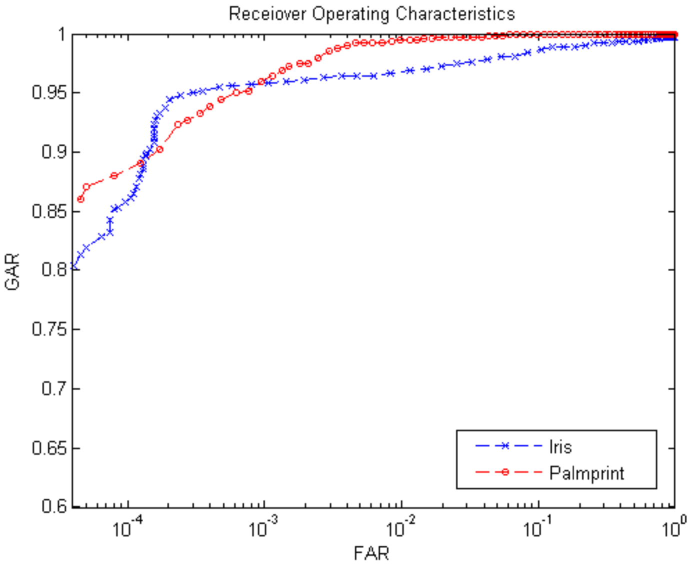
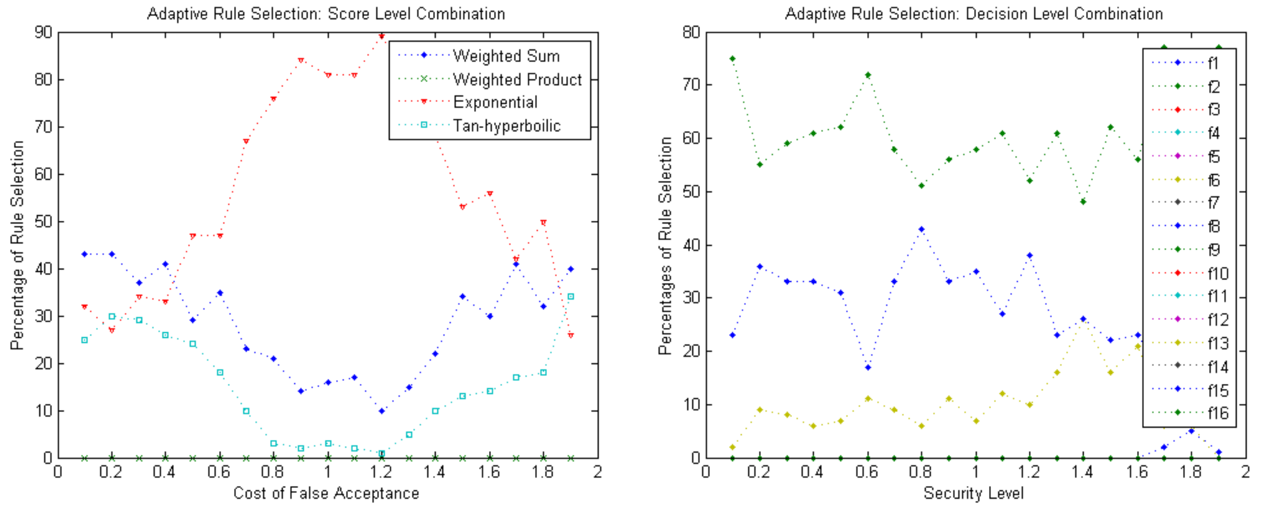
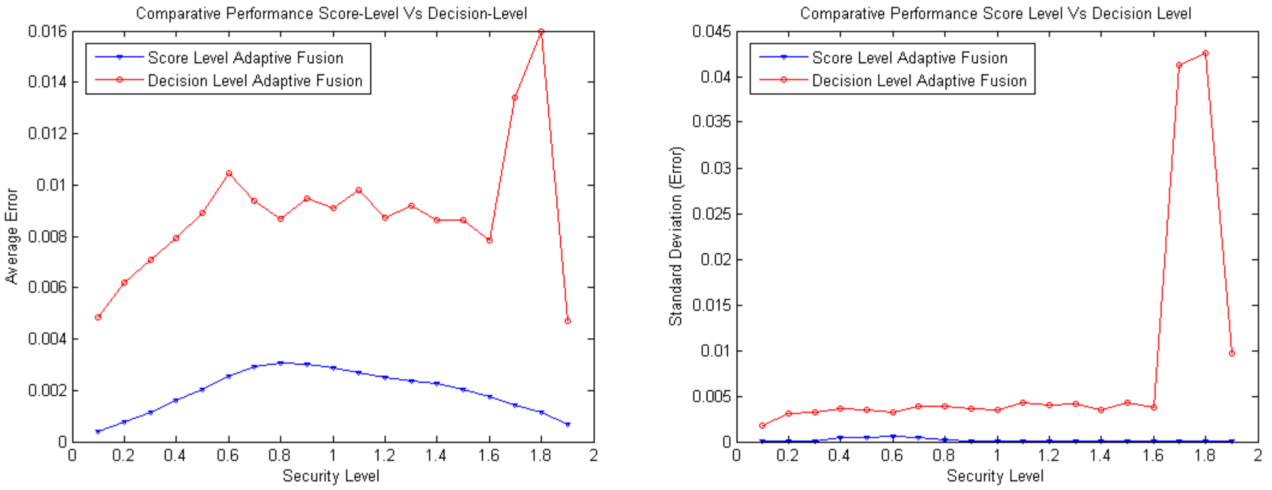


Figure 8: Receiver operating characteristics from the Iris and Palmprint matching scores.



(a) **(b)**

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



(a) **(b)**

Figure 10: Average minimum error in (a) and standard deviation of minimum error in (b) from the score level and decision level approach using the adaptive combination of iris and palmprint modalities

also includes the average of minimum error using the decision-level approach. The comparative results in figure 10 suggests that the dynamic security framework using score level framework achieves minimum average error for each of the chosen cost or desired security level, as compared to the decision level approach in [6]. The summary of experimental evaluation using iris and palm dataset again confirms the effectiveness and the advantages of dynamic security management.

7. Summary and Further Directions

The security level and the traffic flow offered by a multi-biometrics system can be dynamically managed using adaptive combinations of matching scores. The framework illustrated in figure 3 has been experimentally evaluated on the real and simulated biometric data, some of these were discussed in section 6, to ascertain its effectiveness. The experimental evaluations have consistently suggested the superiority of using such score level framework over the decision level based approach. The success of this new framework can be attributed to the usage of score level combinations with accompanying nonlinearities which helps to minimize the weighted sum of errors and also to the usage of PSO which is employed in rather hybrid configuration. The PSO is such configuration is required to optimize the selection of score level combination, its corresponding parameters/weights, and the decision threshold. This PSO shares the majority of the computational requirements of the dynamic multi-biometrics system. However, all such computations with PSO can be performed offline and stored in a look-up-table for the online access and usage. In this chapter, the score level framework suggested in figure 3 has been evaluated on four score level combinations (equation 5). There could be several other score level combination approaches which may perform better, *i.e.*, achieve minimum cost E (equation 1) and can be easily incorporated in the proposed framework. In this context, the likelihood-based score level combination suggested in [25] has shown promising results and could be a potential addition among the score level fusion rules to be considered by PSO.

The dynamic security management using score level combinations has been experimentally evaluated for the bimodal case and further evaluations on large multi-biometrics dataset is required. Another aspect of managing the dynamically changing security requirements is related to the user preferences and constraints/limitations. Therefore further experimental evaluations are required to examine the possibility of employing the alternative biometric modalities, from a given set, while maintaining the desired level of security. There is a range of other open problems that requires the consideration of the user-specific, algorithm-specific, and sensor-specific biometric characteristics, for dynamically managing the multi-biometrics security. The management of dynamic security requirements using the framework discussed in this chapter offers a promising addition in the literature for further multi-biometrics research. However, much more needs to be done before the deployment, of multi-biometrics system that can dynamically ensure the changing security requirements, becomes a reality.

8. References

[1] 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.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] 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.

[11] 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

[12] 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.

[13] NIST BSSR1 biometric score set, http://www.nist.gov/biometricscores

[14] A. Kumar and D. Zhang, "Incorporating User Quality for Performance Improvement in Hand Identification," *Proc. ICARCV 2008*, Hanoi, pp. 1133-1136, Dec. 2008.

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

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

[17] 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.

[18] A. Kumar, "Incorporating cohort information for reliable palmprint authentication," *Proc. 6th Indian Conf. Computer Vision, Graphics, and Image Processing*, Bhubaneswar, India, pp. 583–590, Dec. 2008.

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

[20] 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.

[21] 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.

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

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

[24] S. Tulyakov and V. Govindaraju, "Use of identification trial statistics for combination of biometric matchers*,*" *IEEE Trans. Info. Security Forensics*, vol. 3, no. 4, pp. 719-733, Dec. Jun. 2007.

[19] K. Nandakumar, Y. Chen, S. C. Dass and A. K. Jain, "Likelihood ratio based biometric score fusion,"

IEEE Trans. Patt. Anal. Machine Intell., vol. 30, no. 2, pp. 342-347, Feb. 2008.

[20] N. Poh, R. Wong, J. Kittler, and F. Roli, “Challenges and research directions for adaptive biometric recognition systems,” *Proc. ICB*, Alghero, Italy, June 2009.