An Adaptive Multimodal Biometrics System using PSO

Ola M. Aly
Ministry of Military Production
Egypt, Cairo

Gouda I. Salama
Egyptian Armed Forces
Egypt, Cairo

Tarek A. Mahmoud
Egyptian Armed Forces
Egypt, Cairo

Hoda M. Onsi
Vice dean of post graduate and research, Faculty of Computers and Information Cairo University
Egypt, Cairo

***Abstract*—Multimodal biometric systems which fuse information from a number of biometrics, are gaining more attentions lately because they are able to overcome limitations in unimodal biometric systems. These systems are suited for high security applications. Most of the proposed multibiometric systems offer one level of security. In this paper a new approach for adaptive combination of multiple biometrics has been proposed to ensure multiple levels of security. The score level fusion rule is adapted using (PSO) Particle Swarm Optimization to ensure the desired system performance corresponding to the desired level of security. The experimental results prove that the proposed multimodal biometric system is appropriate for applications that require different levels of security.**

Keywords—multibiometric; match score fusion; PSO; Irsi; Palmprint; Finger_Knuckle

I. INTRODUCTION

The biometric technologies cover a wide range of applications that can be used to verify person identity by measuring human physiological or behavioral characteristics. Biometric characteristics including fingerprint, facial features, iris, voice, signature, and palmprint, finger-knuckle, gait etc. are now widely used in security applications. Unimodal biometric systems perform person recognition based on a single source of biometric information. Such systems are often affected by some problems such as noisy sensor data and non-universality, inter-class similarities, and spoof attacks. Thus, due to these practical problems, the error rates associated with unimodal biometric systems are quite high and consequently it makes them unacceptable for deployment in security critical applications [1].

Some of the problems that affect unimodal biometric systems can be avoided by using multimodal biometric systems. They address the issue of non-universality. It becomes increasingly difficult (if not impossible) for an impostor to spoof multiple biometric traits of an individual. Morever multibiometric systems may also be viewed as fault tolerant systems.

Multibiometric systems which fuse information from multiple biometric sources can be classified into one of six categories [2]: Multi-sensor systems, Multi-algorithm systems, Multi-instance systems, Multi-sample systems, Multimodal systems and Hybrid systems. Depending on the level of information that is fused, the fusion scheme can be classified as sensor level, feature level, score level and decision level fusion. The score level fusion is the most commonly used approach in multibiometric systems.

Most of the multimodal biometric systems proposed in literature have used a fixed combination rule and a fixed threshold to achieve the desired performance. These systems offer a fixed level of security and often have to contend with high false rejection rate if the security level is the highest. Therefore, the performance of these systems is not adaptive to the requirements of the varying level of security [3].

There are wide ranging applications where a biometric system with multiple levels of security is desirable. In this paper, an adaptive multimodal biometric system has been proposed to ensure different levels of security. This system can automatically select the best fusion rule and the optimum decision threshold to achieve the best performance corresponding to the desired security level.

The remainder of this paper is organized as follows: Section (II) describes the related works. Section (III) introduced the proposed multimodal biometric system. Section (IV) introduces the experimental results and discussion. Finally the paper is concluded in section (V).

II. RELATED WORKS

Beginning from 2000, multibiometric recognition systems in score level fusion have gained much attention and several fusion rules have been proposed. Authors in [4] [5] have provided comparisons between fixed and trained rules in combination strategies. It has been shown that the trainable fusion strategies do not necessarily perform better than fixed combination rules.

Sim et al. [6] have proposed an interesting approach to achieve high security using multimodal biometrics. Their approach has involved 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.

Frischholz and Deickmann [7] have developed BioID system which 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 did not provide a systematic way to vary the level of security. Instead, a system administrator made a decision on the decision strategies to be adopted to achieve the desired performance.

Tronci et al. [8] have recently investigated another aspect of multimodal problem that focused on the dynamic selection of matching scores from all the available matching scores. The best matching score from a set of matching scores was selected based on the likelihood of input user being genuine or impostor. However the utility of this approach was quite limited as the achieved performance was not consistent.

Kanhangad et al. [9] have presented a promising approach to the adaptive management of multimodal biometrics to adaptively ensure the desired performance. The authors have proposed an algorithm based on Particle Swarm Optimization (PSO) to optimally combine the individual biometric sensor decisions. The proposed algorithm selected the fusion rule and sensor operating points that minimize a given cost function.

Kumar et al. [10] have introduced an adaptive combination system of multiple biometrics to ensure the optimal performance for the desired level of security using PSO. They have used different biometric combinations (iris, palmprint), (face , speech) and (fingerprint , hand geometry). The experimental results showed that the proposed score-level approach generated fairly stable performance and required smaller number of iterations to generate better performance as compared to the decision level approach.

Anzar and Sathidevi [11] have proposed an efficient PSO integration weight optimization scheme using d-prime statistics to determine the optimal weight factors for the complementary modalities. They have used fingerprint and voice biometrics in the score level fusion. The proposed method has reduced the False Acceptance Rrate (FAR) under varying noise conditions by estimating the optimal integration weight using stochastic optimization technique and Leave-One-Out Cross Validation techniques.

III. THE PROPOSED MULTIMODAL BIOMETRIC SYSTEM

Fig 1 shows the block diagram of the proposed system for optimized matching scores level fusion using Particle Swarm Optimization (PSO). Given three biometrics iris, finger-knuckle and palmprint. The feature vectors are extracted from each biometric separately. Then the matching score for each biometric sample is calculated according to the corresponding templates.

The proposed work is concerned with the development of multimodal biometric system that can dynamically choose from different fusion rules according to the desired level of security. The required level of security is an external parameter that is supplied to the system.

This level of security according to Bayesian sense is quantified by two parameters[10]: (CFA) the global cost of falsely accepting an imposter and (CFR) the global cost of falsely rejecting a genuine user. The Bayesian cost E to be minimized by the multimodal biometric system is the weighted sum of FAR and FRR as shown in eq. 1:

$$E = C_{FA}\, F_{AR}(\eta) + C_{FR}\, F_{RR}(\eta) \qquad (1)$$

Where

$$C_{FA} + C_{FR} = 2$$

Where

$F_{AR}(\eta)$:false acceptance rate

$F_{RR}(\eta)$:false rejection rate

(η): decision threshold

C_{FA} : [0, 1] and C_{FR} : [0, 1]

The main goal of the proposed multimodal biometric system is to minimize the cost function E by selecting the appropriate score level fusion rule and the decision threshold. This is achieved by the Particle Swarm Optimization (PSO) approach.

A. Unimodal biometric systems

1) Iris Identification System

Among biometric technologies, iris-based authentication systems have more advantages than other biometric technologies do. Iris patterns are believed to be unique due to the complexity of the underlying environmental and genetic processes that influence the generation of iris pattern. Iris offers an excellent recognition performance because the false match and false non-match errors are very small [12].

The iris identification system consists of three stages, the first stage is the iris analysis which involves iris localization and iris normalization. The second stage is the feature extraction and encoding. The last stage is the recognition stage which involves identification and verification.

In this paper Daugman's algorithm is used for performing iris localization which is based on applying an integro-differential operator to find the iris and pupil contours [13]. Only the significant features of the iris must be encoded in order to generate the iris code for the matching process. In the proposed system, log-Gabor filter [14] [15] is used for extracting the features from the iris image. Finally matching is performed using the calculated Hamming distance (HD) which is a measure of the number of different bits between the two iris codes[16].

2) Palmprint Identification System

Palmprint based personal identification has become an increasing active research topic over the years. The Palmprint is rich in information not only has the unique information available as on the fingerprint but has far more amount of details in terms of principal lines, wrinkles and creases.

In the proposed Palmprint identification system a preprocessed image database is used, then log-Gabor filter is

performed for extracting the features from the Palmprint image and Hamming distance is calculated during the matching stage [17] [18].

3) Finger-Knuckle Print Identification System

The usage of finger-knuckle biometric for personal identification has shown promising results and generated a lot of interest in biometrics [19]. finger-knuckles of the human hand are characterized by special creases on them. These creases differ from person to another.

In the proposed finger-knuckle identification system, a preprocessed image database is used then the features are extracted from the finger-knuckle image. Linear Discriminant Analysis (LDA) is performed to extract the only significant features from the finger-knuckle image. In this proposed system, the LDA is used to both reducing the dimensionality of the feature vector and performing the classification algorithm. [20] [21].

applied which transforms scores into a common range [0, 1]. The normalized scores are given by [22]:

$$S_i' = \frac{Si - S_{\min}}{S_{\max} - S_{\min}} \qquad (2)$$

Where

S_i' : the normalized matching scores

S_i : the matching scores,

i= 1,2, ….., n and n: number of matching scores

$S_{\min}$ & $S_{\max}$: the min and max match scores

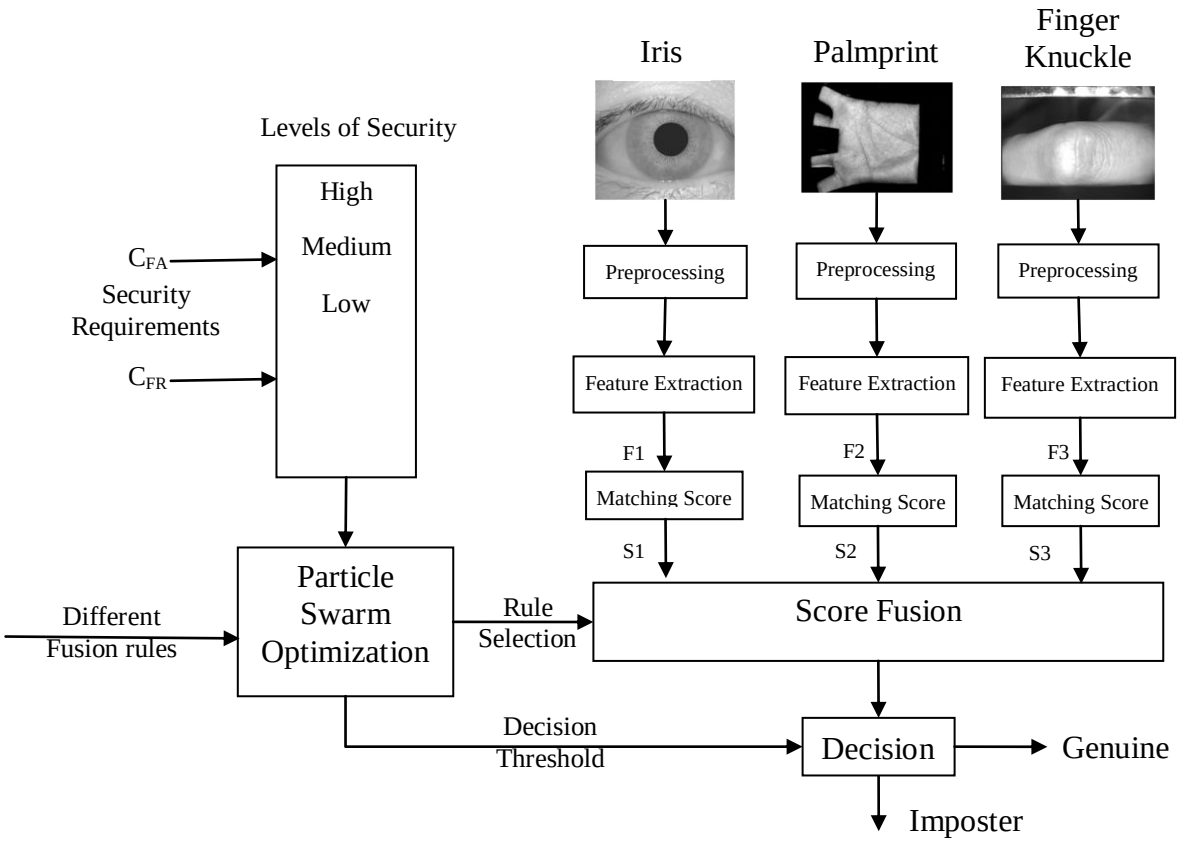

Fig. 1. The block diagram of the proposed system

B. Score Level Fusion

Score level fusion refers to the combination of matching scores provided by the unimodal classifiers in the system. This is the most widely used fusion approach, as evidenced by the experts in the field. But before the fusion step, these matching score should be normalized. In this paper Min-max method is

In order to combine the scores reported by the three matchers, different score level combinations could be applied, such as sum, product, weighted sum rule and min rules:

$$Sum = \sum_{i=1}^{n} S_i \quad (3)$$

$$\Pr oduct = \prod_{i=1}^{n} S_i \quad (4)$$

$$Weighted\ \_Sum = \sum_{i=1}^{n} w_i S_i \quad (5)$$

Where:

N : number of match scores wanted to be fused

S : the matching score

w_i : The weight for each score which calculated as follow

$$W_i = \frac{EER_i}{\sum_{i}^{m} EER_i} \quad (6)$$

Where EER_i is the unimodal biometric error.

m: the number of biometrics.

C. Particle Swarm Optimization (PSO)

PSO is an evolutionary, stochastic, population-based optimization algorithm whose goal is to find a solution to an optimization problem in a search space. The PSO algorithm was developed by Kennedy and Eberhart in 1995 [23]. The main idea of PSO is inspired from the social behavior of organisms, such as birds in a flock. The PSO algorithm imitates the behavior of flying birds and their means of information exchange to solve optimization problems. Each particle (representing a bird in 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 reaching a favorable position.

In a similar manner, the particle in the PSO moves to a new position in the multidimensional solution space depending upon the particle's best position (also referred to as local best position (Pak) and global best position (Pgk). The Pak and Pgk are updated after each iteration whenever a suitable solution is located by the particle (lower cost). The velocity vector of each particle represents/determines the forthcoming motion details. The velocity update equation of a particle of the PSO, for instance (t+1), can be represented as follows[24]:

$$v_{ak}(t+1) = \omega\, v_{ak}(t) + c_1\, r_1\big(p_{ak}(t) - x_{ak}(t)\big) + c_2 r_2\left(p_{gk}(t) - x_{ak}(t)\right) \quad (7)$$

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:

$$x_{ak}(t+1) = x_{ak}(t) + v_{ak}(t+1) \quad (8)$$

Equation (7) indicates that the new velocity of a particle in each of its dimensions depends on the previous velocity and the distances from the previously observed best solutions (positions of the particle). In the implementation of this paper each particle is characterized by three variables; the fusion rule and the decision threshold and the corresponding FAR and FRR for each threshold.

IV. EXPERIMENTAL RESULTS AND DISCCUSION

In this work three different databases for three biometric modalities (iris, palmprint and finger-knuckle) are used. Firstly the results for each unibiomtric system will be presented, and then the results of fusion of two or three biometrics at match score level using PSO will be introduced.

Generally, the performance of the biometric identification system is measured by False Acceptance Rate (FAR) and False Rejection Rate (FRR) or Genuine Acceptance Rate (GAR). The system should have a high GAR with a corrosponding low FAR,FRR and Total Error Rate (TER) [25] [26].

FRR, FAR, GAR and TER are determined as follow:

$$FAR(\%) = \frac{false\ accep\tan ce\ numbers}{No\ of\ imposter\ test} X100\% \quad (9)$$

$$FRR(\%) = \frac{false\ rejection\ numbers}{No\ of\ client\ test} X100\% \quad (10)$$

$$GAR(\%) = 100 - FRR(\%) \quad (11)$$

$$TER(\%) = FRR(\%) + FAR(\%) \quad (12)$$

A. Unimodal Experimental Results

For iris images, CASIA iris Image Database is used [27], includes 2500 iris images from 250 eyes for each eye. 200 persons have been selected, for each person 6 Iris images are used for training and 4 for testing.

For palmprint images, PolyU palmprint database is used [28], contains 7752 grayscale images corresponding to 386 different palms (10 samples for each hand). 200 persons have been selected, for each person we have 6 palmprint images for training and 4 for testing.

For finger-knuckle images, database images introduced in [29] is used, collected from 165 volunteers (12 samples for each user), including 125 males and 40 females. 200 persons have been selected, for each person 8 finger-knuckle images for training and 4 for testing.

Table 1 shows the results of iris, palmprint and finger-knuckle identification systems. It could be noticed that the TER is too much to be suitable for high security applications.

TABLE I. COMPARISON OF UNIMODAL BIOMETRIC RESULTS

Biometric Type	GAR %	FAR %	FRR %	TER %
Iris	**97**	7.14	3	**10.14**
Palmprint	**96.76**	0.00	3.24	**3.24**
Finger_Knuckle	**85.50**	0.00	14.50	**14.50**

B. Matching score fusion results

The goal of this experiment is to evaluate the system performance when using a unimodal biometric system versus a multibiometric system using match score fusion by the aid of PSO as an optimizer.

In this experiment, three score level combinations are considered including sum, product and weighted sum. The PSO is employed to dynamically select the appropriate decision threshold and the best fusion rule to minimize the Bayesian cost for the corresponding required security level. Each particle in PSO is characterized by three variables; a variable representing one of a different score level fusion rules, decision threshold and the corresponding FAR and FRR for each threshold. The performance of PSO is largely depending upon the parameter chosen.

The parameters of PSO in these experiments were determined as follows:

- Population size is 30
- The inertia weight ω is an important parameter as it controls the effect of the previous velocity vector of the swarm on the new one. It is experimentally found that ω in the range [0.8,1.2] yields a better performance [30]. It is selected and fixed at 0.8.
- The acceleration constants c_1, c_2 are set to 1.
- Velocity limitation V_{max} is set to 1.

Table II shows the result of the classification rate including FAR, FRR, TER and GAR for the proposed multimodal biometric fusion approach by the aid of PSO as an optimizer. It is clear that the performance of the proposed multimodal biometric system outperforms the unimodal systems and strongly reduces the TER. The proposed system achieves significant results with best GAR 98.40% and TER 2.60%.

TABLE II. RESULTS OF THEPROPOSED ADAPTIVE MULTIMODAL BIOMETRIC SYSTEMS USING PSO

Biometric Type	GAR %	FAR %	FRR %	TER %
Iris-knuckle-fusion	**98**	0.00	2	**2**
Iris-Palmprint-fusion	**98.40**	1	1.60	**2.60**
Knuckle-Palmprint-fusion	**97.25**	0	2.75	**2.75**

Figs. 2 and 3 show the average of the minimum weighted error rate and the standard deviation of the minimum error of the proposed score level adaptive combination scheme using iris and finger-knuckle modalities. Fig. 4 shows the adaptive rule selected at score level versus the variation of security levels.

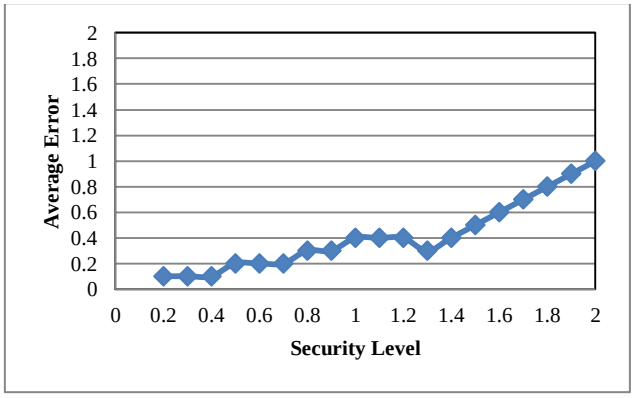

Fig. 2. Average minimum error from the score level approach using the adaptive combination of iris and finger-knuckle modalities

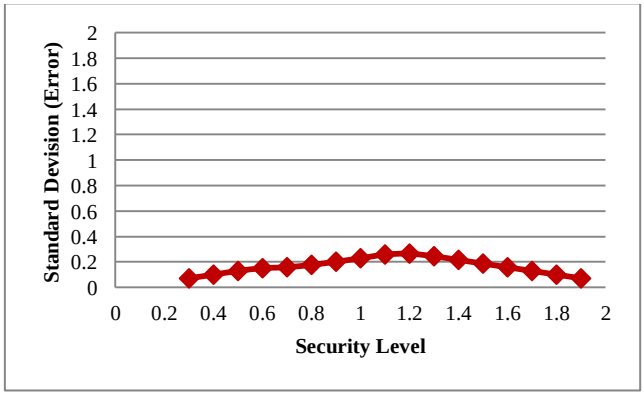

Fig. 3. Standard deviation of the minimum error, from each run, using score level approach for iris and finger-knuckle modalities

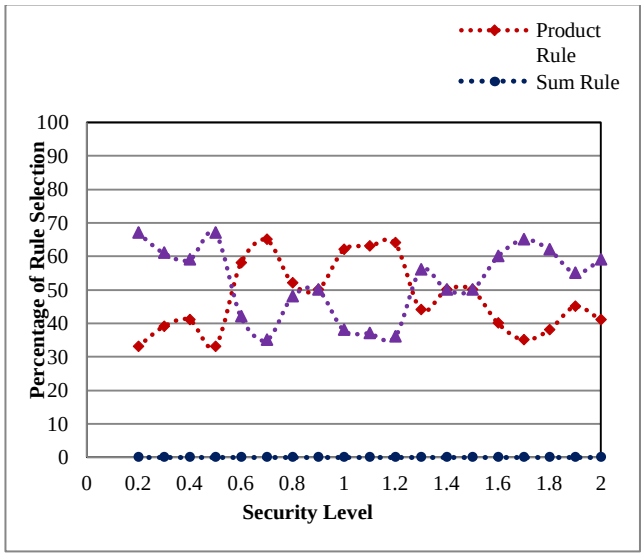

Fig. 4. Adaptive selection of fusion rules using score level combination for iris and finger-knuckle modalities

Figs. 5 and 6 show the average of the minimum weighted error rate and the standard deviation of the minimum error of the proposed score level adaptive combination scheme using iris and palmprint modalities. Fig. 7 shows the adaptive rule selected at score level versus the variation of security levels.

Figs. 8 and 9 shows the average of the minimum weighted error rate and the standard deviation of the minimum error of the proposed score level adaptive combination scheme using finger-knuckle and palmprint modalities. Fig. 10 shows the adaptive rule selected at score level versus the variation of security levels.

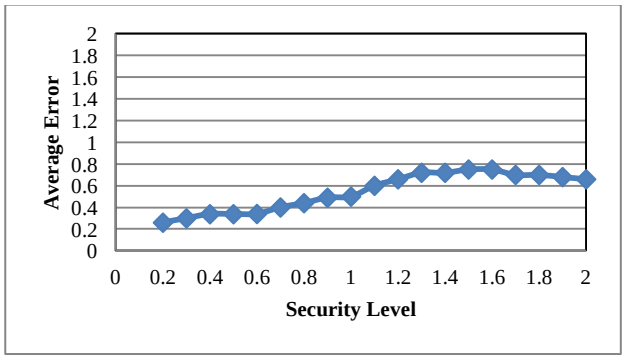

Fig. 5. Average minimum error from the score level approach using the adaptive combination of iris and palmprint modalities

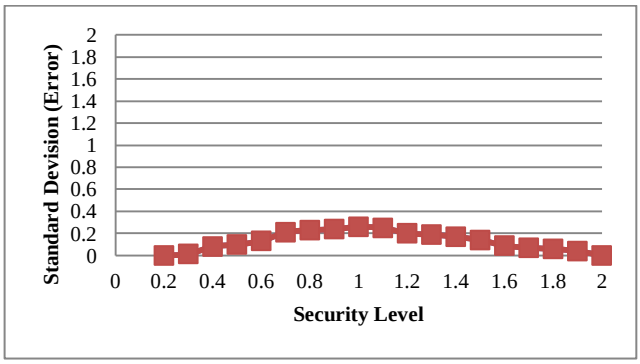

Fig. 6. Standard deviation of the minimum error, from each run, using score level approach for iris and palmprint modalities

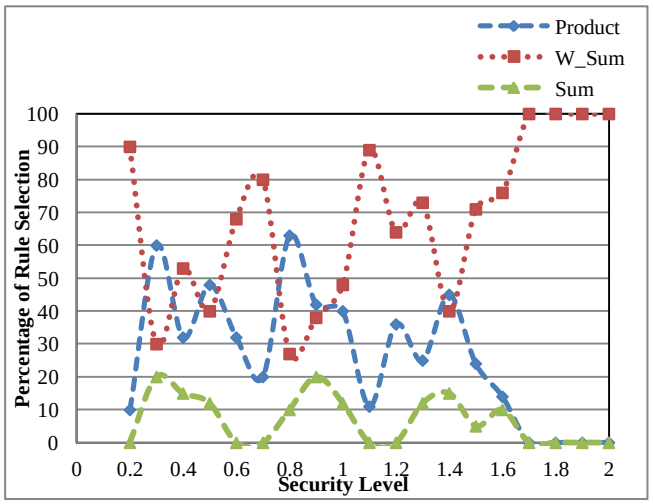

Fig. 7. Adaptive selection of fusion rules using score level combination for iris and palmprint modalities

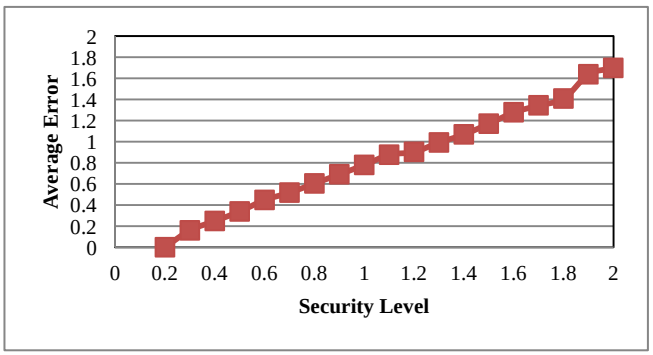

Fig. 8. Average minimum error from the score level approach using the adaptive combination of Knuckle and palmprint modalities

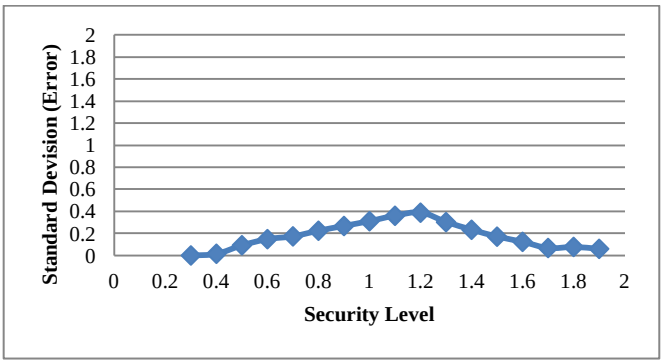

Fig. 9. Standard deviation of the minimum error, from each run, using score level approach for knuckle and palmprint modalities

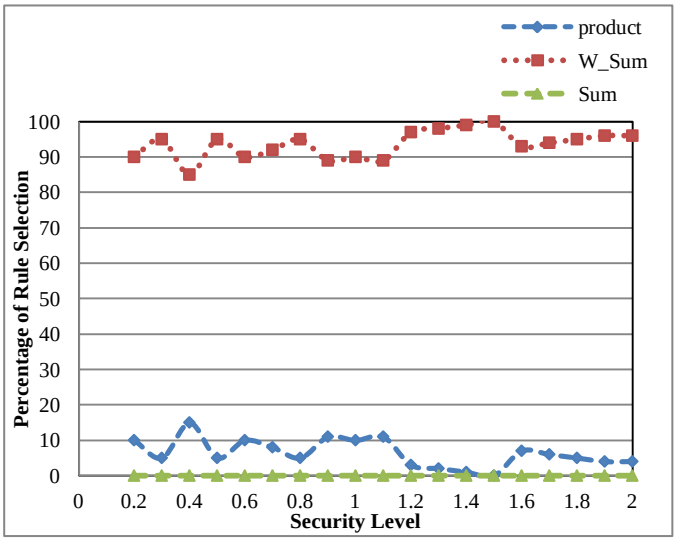

Fig. 10. Adaptive selection of fusion rules using score level combination for knuckle and palmprint modalities

As shown in Figs. 2,5 and 8 the security level is equal to the sum of cost of false acceptance (CFA) and cost of false rejection (CFR). It could be notice that errors increases as the security level is increased from one level to another.

Figs. 3, 6 and 9 shows the standard deviation of the minimum error versus the security level for the score-level fusion approach using different pairs of biometric modalities, It could be observed that the results of the proposed scheme are significantly stable, i.e., have smaller standard deviation, and therefore require significantly smaller number of iterations. From these experiments, it was shown that by using combinations at score-level only ten iterations are adequate to achieve the stable results as compared to the 100 iterations needed in case of decision-level approach [31].

Figs. 4, 7 and 10 show the adaptive rule selected at score level versus the variation of security levels. It can be observed that the sum rule was less choice rul during iterations for any security level. However, the product and weighted sum rules were chosen interchangeably through different levels of security.

V. Conclusion

In this paper, a new multimodal biometric identification system is proposed using three modalities including iris, palmprint and finger-knuckle with fusion at matching score level. The main objective of this work is to develop a reliable approach for the adaptive combination of multiple biometric modalities to ensure desired level of security. The proposed method uses PSO to achieve adaptive combination of multiple biometrics from their matching scores.

The PSO is used to optimize the selection of score level combination, its corresponding parameters, and the decision threshold. In this work only 3 fusion rules have been suggested, there may be several other score level combination approaches which may perform better, i.e., achieve minimum cost E and can be easily incorporated in the proposed framework. The experimental results shown in Figs. 4, 7 and 10 illustrate the dynamic rule selection of these score level combinations to ensure the desired level of security.

The results prove that the proposed multimodal biometric system improves the identification rate and outperforms the unimodal biometric systems using different biometric combinatioins. Morever, the TER is strongly decreases to 2.60% at 98.4% Identification rate.

References

[1] F. Wang and J. Han, “Robust multimodal biometric authentication integrating iris, face and palmprint”, Information Technology and Control, vol.37, no.4, pp. 326-332, 2008.

[2] A. Ross, K. Nandakumar and A. Jain. Handbook of Multibiometrics1st edition. Springer, New York, USA, 2006.

[3] A. Kumar, V. Kanhagad and D. Zhang, “A new framework for adaptive multimodal biometrics management”, IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, March 2010

[4] D. Tax, M. Breukelen, R. 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. Marcialis, “An experimental comparison of fixed and trained fusion rules for crisp classifier outputs,” Intl. Workshop on Multiple Classifier Systems, Cagliari, Italy, Jun. 2002.

[6] 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.

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

[8] R. Tronci, G. Giacinto and F. Roli, “Dynamic score selection for fusion of multiple biometric matchers”, Proc. 14 IEEE International Conference on Image Analysis and Processing, Modena, Italy, pp. 15-20, 2007.

[9] 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, 2008.

[10] A. Kumar, , V. Kanhangad and D. Zhang, “ A new framework for adaptive multimodal biometrics managemen”, IEEE Transactions on Information Forensics and Security, vol. 5, pp. 92-102, Mar. 2010

[11] S. Anzar and P. Sathidevi, “An efficient PSO optimized integration weight estimation using D-prime Statistics for a multibiometric system”, International Journal on Bioinformatics & Biosciences (IJBB) vol.2, no.3, September 2012.

[12] J. Daugman “How iris recognition works”, IEEE Trans. On Circuits and Systems for Video Technology. vol. 14, no. 1, pp. 21-30. 2004.

[13] J. Daugman, “High Confidence Visual Recognition of Persons by a Test of Statistical Independence,” IEEE Trans. Pattern Anal. Machine Intell, vol. 15, pp. 1148-1161, 1993

[14] D.Gabor, " Theory of communication ", J. Inst. Elect. Eng. London, Vol. 93, No. 3, 1946.

[15] A. Kumar and A. Passi, "Comparison and Combination of Iris Matchers for Reliable Personal Authentication," Pattern Recogniion., Vol. 23, No. 3, pp. 1016–1026, March 2010.

[16] L. Ma, T. Tan, Y. Wang and D. Zhang, "Efficient Iris Recognition by Characterizing Key Local Variations", IEEE Transactions on Image Processing, Vol. 13, No. 6, pp739-750, June 2004.

[17] R. Chu, Z. Lei, Y. Han and S. Li," Learning Gabor magnitude features for palmprint recognition", ACCV, pp. 22–31, 2007.

[18] A. Kong, "Palmprint Identification Based on Generalization of IrisCode", PhD Thesis, University of Waterloo, Canada, 2007.

[19] A. Kumar and C. Ravikanth, "Personal authentication using finger knuckle surface", IEEE Trans. Information. Forensics & Security, vol. 4, no. 1, pp. 98-110, March 2009

[20] H. Yu and J. Yang, "A direct LDA algorithm for high dimensional data with application to face recognition," Pattern Recognition, September 2001.

[21] P. Navarrete and J. Ruiz-del-Solar, "Analysis and Comparison of Eigenspace-Based Face Recognition Approaches," International Journal of Pattern Recognition and Artificial Intelligence, vol. 16, no. 7, November 2002.

[22] A. Pour, K. Faez, and R. Amirfattahi "Multimodal biometric system using face, ear and gait biometrics", 10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010).

[23] J. Kennedy and R. Eberhart, "Particle swarm optimization". IEEE Int'l Joint Conf. on Neural Networks, Perth, Australia. (1995).

[24] 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.

[25] T. Sabareeswari and S. Stuwart," Identification of a Person Using Multimodal Biometric System", International Journal of Computer Applications vol. 3, no.9, 2010.

[26] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification", IEEE Trans. Pattern Anal. Mach. Intell. , Vol. 20, No. 12, pp. 1295– 1307, 1998.

[27] Chinese Academy of Science Institute of Automation, Database of the Eye Grayscale Images. http://www.sinobiometrics.com

[28] PolyU Palmprint Database, http://www.comp.polyu.edu.hk/~biometrics/

[29] L. Zhang, "Finger-Knuckle-Print: A new Biometric Identifier", ICIP, Cairo, Egypt, 2009.

[30] Y. Shi and R.C. Eberhart, "A modified particle swarm optimizer", proc. IEEE conference on evolutionary computation, 1998.

[31] K. Veeramachaneni, L. Osadciw and P. Varshney, "An Adaptive Multimodal Biometric Management Algorithm," IEEE Trans. Sys. Man & Cyber., vol. 35, no. 3, pp. 344-356, August 2005.