A Grid-based Neural Network Framework for Multimodal Biometrics

Sitalakshmi Venkataraman

Abstract**—**Recent scientific investigations indicate that multimodal biometrics overcome the technical limitations of unimodal biometrics, making them ideally suited for everyday life applications that require a reliable authentication system. However, for a successful adoption of multimodal biometrics, such systems would require large heterogeneous datasets with complex multimodal fusion and privacy schemes spanning various distributed environments. From experimental investigations of current multimodal systems, this paper reports the various issues related to speed, error-recovery and privacy that impede the diffusion of such systems in real-life. This calls for a robust mechanism that caters to the desired real-time performance, robust fusion schemes, interoperability and adaptable privacy policies.

The main objective of this paper is to present a framework that addresses the abovementioned issues by leveraging on the heterogeneous resource sharing capacities of Grid services and the efficient machine learning capabilities of artificial neural networks (ANN). Hence, this paper proposes a Grid-based neural network framework for adopting multimodal biometrics with the view of overcoming the barriers of performance, privacy and risk issues that are associated with shared heterogeneous multimodal data centres. The framework combines the concept of Grid services for reliable brokering and privacy policy management of shared biometric resources along with a momentum back propagation ANN (MBP-ANN) model of machine learning for efficient multimodal fusion and authentication schemes. Real-life applications would be able to adopt the proposed framework to cater to the varying business requirements and user privacies for a successful diffusion of multimodal biometrics in various day-to-day transactions.

Keywords**—**Back Propagation, Grid Services, Multimodal Biometrics, Neural Networks.

I. INTRODUCTION

AN artificial neural network (ANN) has the ability of reasoning and learning, emulating human brain, and is made up of many artificial neurons that operate in parallel [1][2]. In recent years, ANN models are being experimented in biometric human identification system by exploiting their inherent capacity to learn and generalise [3][4][5]. The advantage of neural network based machine learning over other approaches including statistical models is that the ANN does not require prior knowledge of statistical distribution of data nor any influence parameter on data sources to be specified. Hence, the most popular ANN model, namely, the back-propagation ANN (BP-ANN) is ideally suited for multi data source applications [6][7][8]. Since biometric systems rely on multiple data sources that include fingerprints, face, iris, DNA, gait, voice, signature, etc. for a more reliable personal identification [9], introducing momentum back-propagation ANN improves the accuracy [10]. However, in order for biometrics to be successful, such advanced systems should also be able to deal with privacy concerns, multimodal biometric fusion issues, distributed resource sharing and more importantly real-time accuracy [11][12].

Most real-life biometric systems are still unimodal, i.e. they depending on only single biometric trait such as fingerprint and they are faced with a variety of problems as listed below:

i) Noise and permanence – Biometric data may be required to be revoked and reissued due to noisy data or changes in the person's features due to factors such as aging / deformity and even due to security breach that result in incorrect identification of a person [12].
ii) Multiple trait variations - Different biometric technologies are at different stages of maturity and lead to intra-class and inter-class variation issues and overlaps [13].
iii) Individual privacy – User confidence in biometrics is based on whether the system allows exchange of biometric data with other databases that could lead to function creep [14].
iv) Real-time accuracy – The biometric feature space of multiple users grows tremendously and this affects the verification rate and the overall performance of the system [15].

Some of these unimodal issues in biometric systems can be overcome by multimodal biometrics as they provide multiple source of identity evidence to address noisy data, identity spoofing and class variations [16][17]. User acceptance, privacy, speed and accuracy still pose main problems for multimodal biometrics. Current research investigations in ANN models may provide promising improvements in reliability and efficiency related issues [15]. However, such systems would require advanced biometric technology interfaces and policy framework that can address performance, security adaptability and privacy issues for a successful adoption in everyday life [18]. Generally, the main limitations of the present systems that use multimodal biometrics are: a) fixed calibration that does not adapt to different user / application / service requirements, b) lack of interoperability among multiple distributed heterogeneous environments, c) shared resources issues, and d) poor data optimisation leading to low quality of service (QoS).

In this paper, the proposed Grid-based neural network framework for multimodal biometrics has the main objectives of i) scalability and flexibility to deal with different biometric requirements, ii) seamless integration of distributed

Dr. Sitalakshmi Venkatraman is with the Graduate School of Information Technology and Mathematical Sciences at University of Ballarat, PO Box 663, Ballarat, VIC 3353, Australia; phone: 61-3-5327-9074; fax: 61-3-5327-9289; e-mail: s.venkatraman@ballarat.edu.au.

heterogeneous systems, iii) sharing of resources catering for different privacy levels, and iv) improving real-time accuracy. Since the learning in ANN is based on the training adequacy and the generalisation is based on the structure of the neural networks, this paper presents Momentum Back Propagation ANN (MBP-ANN) approach that is capable of achieving very high levels of accuracy in biometric identification. Also, the proposed Grid-based framework that provides scalability, security and high-performance features to the distributed and heterogeneous resources [19] [20], offers promise to overcome the aforesaid limitations of the current unimodal and multimodal biometric systems.

Section II provides the multimodal fusion issues that warrant a highly accurate multimodal identification system. Section III describes the MBP-ANN approach to achieve the desired high level of reliability and accuracy. Section IV presents the Grid-based neural network framework for achieving the required real-time performance, scalability, distributed resource sharing and security with multimodal biometric systems. Finally, Section V summarises this ongoing research work along with future work.

II. Fusion Issues in Multimodal Biometrics

In multimodal biometrics, the multiple biometric data used to establish a person's identity could be based on the following modalities: a) multiple samples (e.g. fingerprints of the same finger – rolled or flat), b) multiple instances (e.g. left and right retina), c) multiple forms (e.g. polar and normalised forms of iris), and d) multiple traits (e.g. fingerprint, gait and DNA). Each of these modalities (Fig. 1) when used could pose various issues with regard to fusion of the multiple biometric data [21]. The fusion method could be adopted at the feature level (before conducting the matching) or at the rank and score level (after performing the matching).

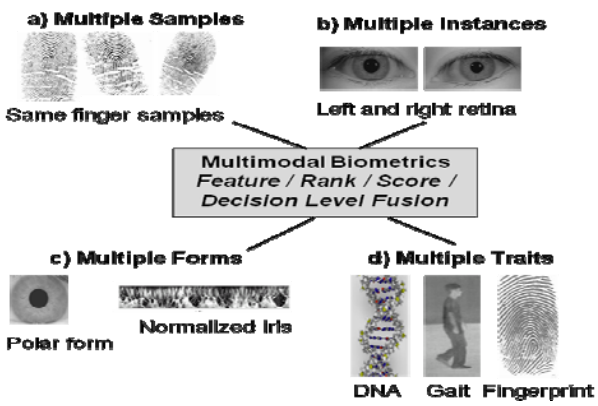

Fig. 1. Fusion types in multimodal biometrics

Fusion issues arise at the time of enrolment, identification and generalisation of multimodal biometric data. A fusion method takes in multiple biometric data that is available in any combination of the above modes to arrive at a conclusion based on the combined evidence. It requires a mechanism to identify duplicates and association of multimodal biometrics identities of the same person. An example multimodal identification and fusion of scores of multiple fingerprint samples of the same person is demonstrated in Fig 2. Here, the fusion is performed after matching the two fingerprint samples taken from the same finger (with different orientation) and the generalised scores are derived after identifying that they both (duplicates) belong to the same person.

Fig.. 2. An example post-matching fusion of scores (multiple samples)

On the other hand, in the case of multiple instances of the same biometric trait, the features are extracted and a combined feature could be generated before matching. An example multimodal identification and fusion of features taken from multiple instances of a person's face (with / without spectacles and different lighting source) is demonstrated in Fig 3. A matching threshold of 1% is assigned here for the fusion.

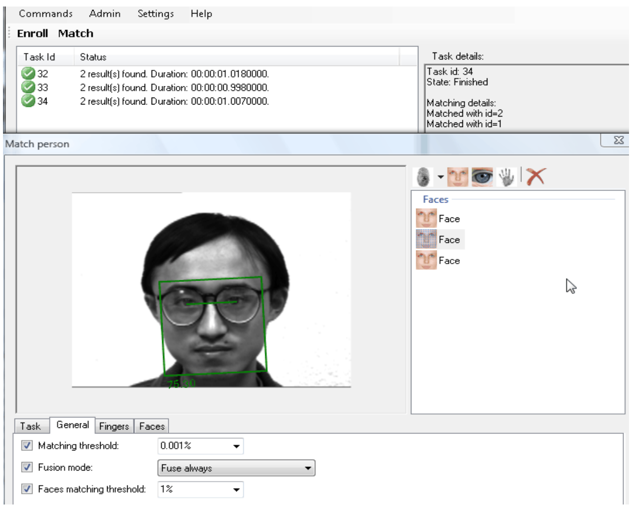

Fig. 3. An example pre-matching fusion of features (multiple instances)

These experiments that were conducted with biometric traits taken from various public domain databases [22][23] clearly indicate that one of the main issues that contend multimodal biometrics is in dealing with complex and non-universal fusion methods. Many fusion methods could be adopted to combine the modalities at the feature level (pre-matching stage) [24][25] or at the matching / post-matching (decision) levels [26][27]. Some fusion modules adopt rule-based approaches that combine score calculations [28], while some adopt machine learning approaches that range from statistical models to neural network models [29]. A highly complex fusion technique may offer accuracy for large scale multiuser applications but would take more time to optimise and would eventually degrade the system performance [30]. Neural networks could provide considerable improvement in performance as many artificial neurons operate in parallel and have the capability of learning and generalisation. The next section describes the Momentum Back Propagation ANN model adopted in this paper.

III. Momentum Back Propagation ANN Model

An ANN has a parallel distributed processing architecture of nodes, called neurons, and connections, called weights and biases [1][2]. A multilayered ANN typically consists of input nodes (x), hidden nodes (z) and output nodes (y). Learning in neural network takes place by changing the weights (w) and biases (b) of the network so as to minimize the error. For single-layered network, the relationship of these variables is given by the following formula:

$$y_i = f\left(\sum_{j=1}^{m} w_{ij} x_j + b_i\right)$$

The most commonly used neural network learning approach is the back propagation method that computes and propagates the error backwards through the network starting at the output nodes [8][10]. The activation function uses the sigmoidal function as given below:

$$g(x) = \frac{1-e^{-x}}{1+e^{-x}}$$

The error (E) is calculated as the difference between actual (y) and desired (d) output values and the square of error calculated is given as:

$$E = \sum_{i=1}^{p}\sum_{j=1}^{m}[d_j(k) - y_j(k)]_i^2$$

With p number of training patterns and m number of output nodes, the stopping criteria for the training would be when the error is very small at each learning step (k). With the learning rate as η, the additional momentum expression (momentum rate α) is introduced in the weights to speed up the convergence rate and to hold weights history of previous changed weights as follows:

$$w_{ij}(k+1) - w_{ij}(k) = \eta\delta_j(k)y_i(k) + \alpha[w_{ij}(k) - w_{ij}(k-1)]$$

Recent research studies [10][30] with face, speech and fingerprints indicate that the additional momentum in MBP-ANN have aided in improving the verification rate considerably and in reducing the false acceptance rate (FAR) down to 0.0001%. Hence, this research adopts a MBP-ANN model as described above. Various biometric traits could be trained to render high levels of accuracy through the learning modules of the MBP-ANN model at the enrolment, feature extraction and authentication processes where FRR (false rejection rate) and FAR (false acceptance rate) could be minimised. An example scenario that uses the MBP-ANN model for the fusion of multiple modalities (multiple samples, multiple instances, multiple forms and multiple traits) is given in Fig 4.

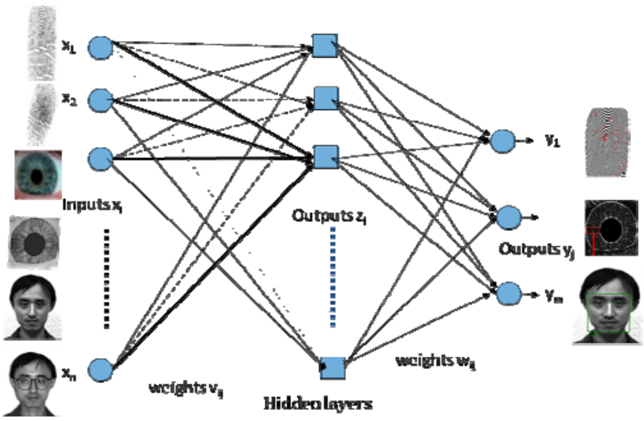

Fig. 4. MBP-ANN model for multimodal biometric fusion

The MBP-ANN model described here could be used at the enrolment stage to generate a collection of generalised features as output for various biometric traits with high level of accuracy and speed gained through momentum back propagation. These features could be analysed and combined into single generalised feature collection that is stored into the database as templates. By maintaining history of changed weights in the hidden layers of the back propagation learning, the MBP-ANN ensures that the enrolled features are more reliable and accurate in a quick way. Similarly, at the time of verification, the MBP-ANN compares the biometric inputs (multiple in the case of multimodal) with the pre-stored template collection and uses the MBP learning modules for a faster fusion and accurate identification.

Having addressed the reliability and accuracy issues of multimodal biometrics through MBP-ANN learning algorithms, the next main challenge is to address the acceptability of multimodal biometrics in large-scale applications that warrant real-time performance, scalability, distributed resource sharing and security / privacy requirements in multi-user environments. Most of the commercially available multimodal systems present proprietary systems, which are not interoperable and do not support sharing of resources in real-life distributed multi-user environments [31]. The Grid, which provides a means for sharing resources with the main focus of high performance computing, forms an ideal solution. Grid information services are capable of adaptability and handling of data sets and neural networks homogenously. The Grid information service could match the user-centric preferences of the biometric traits with the business transaction requirements towards addressing the privacy and security risk issues, thereby paving way for flexibility, scalability and user-acceptance. The next section presents a Grid-based neural network framework for multimodal biometric systems. Using such a framework, the weakness of any biometric ANN classifier could be compensated by other stronger biometric ANN classifiers through the distributed Grid service. This way, Grid-based biometric systems could achieve even higher accuracy levels and reliability of multimodalities in a collaborative and flexible manner that could be tuned to the changing business and user requirements.

IV. Grid-based MBP-ANN Framework for Biometrics

A Grid is a collection of distributed services that offer technological and organizational interaction for users or business applications to interact for their data processing services [9][32]. This section proposes a Grid-based MBP-ANN framework that could cater to the information services for various multimodal biometric users and applications. Typically, a Grid consists of certain basic and advanced functions that are inherent features of Grid information services. These are listed below and could be leveraged for processing multimodal biometric transactions:

Discovery and Brokering: This functionality helps in the discovery of biometric resources and brokering of different biometric fusion schemes in the discovered resources.

Data Sharing: This feature allows access to very large databases of biometric data and other personal identification data in a distributed and shared fashion. Other data services such as metadata cataloguing, data caching, data replication, backup and storage services are also essential aspects for biometric transactions.

Monitoring: The multimodal biometric processing is to be monitored closely to detect misuse/ intrusions, and to check that the matching schemes are applied reliably over large databases. A good matching should avoid false positives and false negatives and at the same time inter-operate on different types of biometric traits with different noise levels.

Policy controlling: This feature controls the access mechanisms for the biometric databases and the rules for notification processes as well.

Security: Grid information services are capable of providing the security controls for multiple distributed infrastructures and the privacy, authentication, authorisation and accounting mechanisms required for processing biometric data. The capability of Grid information services with dynamic instantiation of security protocols and services provide an advanced biometric functionality.

Resource Management: This facility involves dynamic scheduling, load balancing, workflow management, fault tolerance and error recovery of biometric systems transacting in distributed Grid environments.

The proposed Grid-based framework uses a momentum back propagation method of artificial neural network (MBP-ANN) for incorporating multimodal biometric fusion schemes within the requested biometric information services. It provides the flexibility at the client services layer for both users and business transactions to choose the suitable biometric modalities that are compatible with the user-preferred and transaction-specific risk levels that are assigned for different business applications. An overview of the framework is depicted in Fig. 4, which shows the four main layers and their major components. These layers and the multimodal biometric information processing performed from the top layer to the bottom layer are described next.

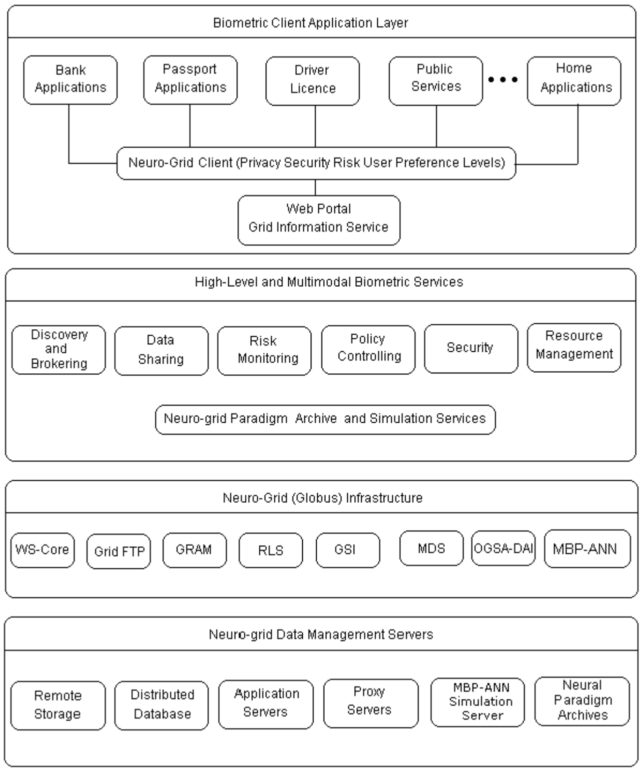

Fig. 4. Grid-based MBP-ANN framework for multimodal biometrics

A. *Biometric Client Application Layer*

This top layer consists of a Web portal, which provides a user-friendly and browser-based interface for the users and businesses to make use of the Discovery and Brokering features of Grid services for finding the suitable biometric resources for their biometric authentication transactions. It allows different businesses, government and home applications, such as, bank applications, e-passport services, driver licence applications, e-shopping, and public services (e.g., community, library and transport), to setup their biometric requirements and neural network parameters, that serve as inputs to the next level of Grid service. This layer also includes Neuro-Grid client for the users to determine their multimodality preferences to undergo MBP-ANN trained fusion for different applications that are based on the risk and privacy levels associated with those biometric-enabled transactions. The portal uses such user-centric and application-specific varying parameters to match their requirements in order to associate the appropriate biometric metadata and datasets that are utilized in the next layer. This facilitates the identification of their resource locations for subsequent data retrieval and processing.

B. *High-level and Multimodal Biometric Services*

In this second layer of the Grid-based framework, the high-level Grid services provide the capabilities of reliable data movement, cataloguing, metadata access, data subsetting and aggregation. Such high-level data features form the sub-components that are based on the Open Grid Services Architecture Data Access and Integration (OGSA-DAI) service, which uses the Replica Location Service (RLS) to retrieve the location information from the distributed RLS databases [33]. This layer provides the Neuro-Grid paradigm and simulation services for mapping the inputs with metadata that is required for processing the multimodal biometrics. The Neuro-Grid paradigm and simulation services determine the archive data rules and adaptive fusion rules that are required for training and processing the MBP-ANN in the next layer.

C. Neuro-Grid (Globus) Infrastructure

This layer provides remote, authenticated access to shared data resources such as biometric data, risk-based and neurbased metadata through Meta Directory Services (MDS), and other services such as RLS and transaction management services. This is accomplished by the Grid Security Infrastructure (GSI) for secure authentication. It provides the flexibility of using data hiding techniques, encryption and one-time templates based on the level of privacy and risk specified by users and biometric transactions. A shared data access could be incorporated for integrating shared authorisation service for both group-based and individual access to datasets through GridFT [34]. Apart from enforcing data encryption through GSI, reliability could also be enhanced through the monitoring infrastructure by using Globus Toolkit's Grid information services [35]. The Grid Resource Allocation and Management (GRAM) sub-component provides the necessary service to communicate between the multimodal biometric recognition module provided by the MBP-ANN model and the Grid services modules to access and process biometric data.

D. Neuro-Grid Data Management Servers

This is the lower-most layer of the Grid architecture consisting of all the computational resources such as Web servers, application servers, database servers, neural simulation servers, neural paradigm archives and mass storage systems including CPU, cache, buffers, etc. This lowest layer provides scalable, dependable and secure access to the distributed resources that is required for biometric applications as Grid computing maintains administrative autonomy and allows system heterogeneity. The database servers are used to store metadata, biometric features, privacy policy rules, etc. The application servers are for running the Open Grid Services Architecture (OGSA) applications or legacy applications (non-OGSA) such as servlets running in Java application server containers, neural network servers running the training simulators, and the Web servers for hosting the Internet portal services for the different biometric applications. The neural simulation servers consist of the MBP-ANN model for biometric feature extraction and the MBP learning mechanisms for using appropriate multimodal fusion adoption scheme that match with the required privacy and risk policy of the transaction. The fusion adoption scheme determines the best of the available algorithms that are configured through machine learning and training to suit each particular biometric-enabled business transaction. Such training mechanisms have been successfully adopted, especially in speech processing [36]. The MBP-ANN model also supports cancellable and re-issuable biometrics. If a particular biometric trait (or sample or instance or form) or even a variant of transformed biometric is distorted or compromised, that particular representation could be cancelled and re-issued by generating the biometric data with a new transform. This is possible because the MBP training paradigms maintain histories and are preserved as archives of the machine learning process for future references. This way, MBP-ANN could improve user acceptability and market penetration of multimodal biometrics. In summary, this layer provides all the necessary resources and the computational power to the end-users for successfully adopting multimodal biometrics in various secured real-life applications.

In a nutshell, the above Grid-based framework could be adopted in real-life applications as the Globus infrastructure offers an open source collection of Grid services that follow standard OGSA architectural principles. Organisations and users could register with Globus for a certificate to deploy and make use of Grid services at their servers and local computer machines. This research project uses the Grix tool to configure proxy and biometric models for working with Web services of Globus Grid portal (Fig. 5).

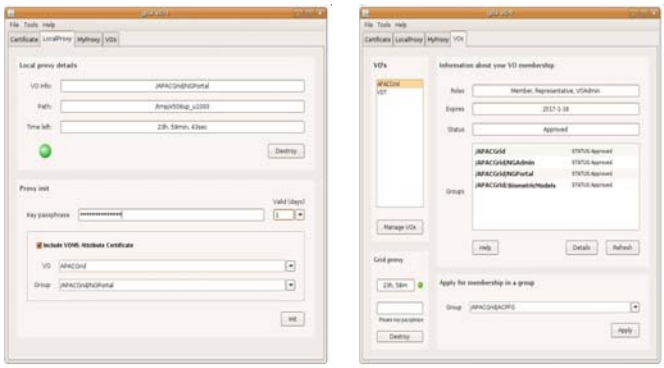

Fig. 5. Configuration of proxy and biometric models on Globus Grid portal

V. CONCLUSIONS AND FUTURE WORK

While the design of multimodal biometric systems have been researched and developed over the last few decades to overcome the limitations of unimodal biometrics, their adoption is still slow in real-life applications. Based on studies performed on current systems, this paper describes the various issues that face multimodal biometrics and argues the need for a mechanism that ensures high performance, interoperability, scalability and more importantly, privacy and security in order to achieve user acceptance and market penetration. This warrants a framework with capabilities such as, advanced data access of heterogeneous biometrics, sophisticated multimodal fusion algorithms and adaptive privacy schemes.

With the above prime motivation, this paper has proposed an artificial neural network (ANN) model that is based on momentum back propagation (MBP) learning method along with the concept of Grid-based information services for deploying multimodal biometrics in real-life applications. Such a Grid-based neural network framework that uses momentum back propagation for multimodal biometric fusion and authentication is capable of taking advantage of Grid services for seamless integration and information sharing among large, heterogeneous and distributed multimodal data centres. Further, by combining with the MBP-ANN model, the proposed framework caters to real-time performance and accuracy of complex fusion schemes, user-centric privacy policy schemes and adaptable risk schemes that have recovery mechanisms for cancelling and re-issuing multimodal biometric identities. These compelling advantages of the Grid-based MBP-ANN framework would pave way for a better diffusion of multimodal biometrics in everyday life applications.

REFERENCES

[1] S. Haykin, *Neural Networks – A Comprehensive Foundation*. McMillan, New York, 1994.

[2] I. Cloete and J. M. Zurada (Eds.), *Knowledge-Based Neurocomputing* MIT Press, Cambridge, Massachusetts, 2000

[3] H. Lee, S. Hong and E.Kim, "Neural network ensemble with probabilistic fusion and its application to gait recognition", *Neurocomputing*, Vol. 72 , No. 7-9, pp. 1557-1564, 2009.

[4] M.Alvarado, P.Melin, M.Lopez, A. Mancilla, and O. Castillo, "A hybrid approach with the wavelet transform, modular neural networks and fuzzy integrals for face and fingerprint recognition", *Journal of Current Development in Theory and Applications of Wavelets*, Vol. 1, No. 2, pp.235–250, 2007.

[5] J. Urias, D. Hidalgo, P Melin and O. Castillo, "A method for response integration in modular neural networks with type-2 fuzzy logic for biometric systems", in *Analysis and Design of Intelligent Systems using Soft Computing Techniques*, Patricia Melin et al. (eds.), SpringerVerlag, Germany, No. 1, pp.5–15, 2007.

[6] J.: Devillers, *Neural Network in QSAR and Drug Design*.Academic Press, San Diego, CA, 1996.

[7] R. Fu, T. Xu, Z.: Pan, "Modeling of the Adsorption of Bovine Serum Albumin on Porous Polyethylene Membrane by Backpropagation", *Artificial Neural Network. Journal*, Membrane Science Vol. 251 pp. 137-144, 2004.

[8] Y. Chauvin and D. Rumelhart (Eds), *Backpropagation: Theory, Architectures and Applications*. Hillsdale, NJ:Lawrence Erlbaum Associates, 1995.

[9] A. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology", *Special Issue on Image and Video-based Biometric*s, Vol. 14, No. 1, pp. 4-20, 2004.

[10] C. Park, M. Ki, J. Namkung, and J.K. Paik, "Multimodal Priority Verification of Face and Speech Using Momentum Back-Propagation Neural Network" In *Lecture Notes in Computer Science*. ISNN (2), Vol. 3872, pp. 140-149, 2006.

[11] S. Venkatraman, and S. Kulkarni, "The Impact of Biometric Systems on Communities: Perspectives and Challenges", *Proceedings of 11th Annual Australian Conference on Knowledge Management and Intelligent Decision Support - ACKMIDS08*, 2008.

[12] R. Ryan: The importance of biometric standards. *Biometric Technology Today*, 17(7):7-10, 2009.

[13] M.C. Fairhurst, and M.C.C. Abreu, "Balancing Performance Factors in Multisource Biometric Processing Platforms". IET Signal Processing, Vol. 3, No. 4, pp. 342-351, 2009.

[14] W. Sheng, G. Howells, M.C. Fairhurst, F. Deravi, and K. Harmer, Consensus Fingerprint Matching with Genetically Optimised Approach. Pattern Recognition, Vol. 42, No. 7,. pp. 1399-1407, 2009.

[15] N. Goranin and A. Cenys, "Evolutionary Algorithms Application Analysis in Biometric Systems", *Journal of Engineering Science and Technology Review* Vol. 3, No. 1, pp. 70-79, 2010.

[16] A. Jain and A. Ross, "Multibiometric Systems", *Communications of the ACM*, Vol. 47, No. 1, pp. 34-40, 2004.

[17] M. De Marsico, M. Nappi, D. Riccio, G. Tortora, "A Multiexpert Collaborative Biometric System for People Identification", *Journal of Visual Languages & Computing*, Vol. 20, No. 2, pp. 91-100, 2009.

[18] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multi-biometric Templates Using Fingerprint and Voice", *Proceedings of SPIE Conference on Biometric Technology for Human Identification*, 2008.

[19] A. Shoshani, A. Sim, and J. Gu, "Storage Resource Managers: Essential Components for the Grid", In *Grid Resource Management: State of the Art and Future Trends*, J. Nabrzyski, J. Schopf, and J.Weglarz, Eds. New York: Kluwer, 2003.

[20] Venkatraman, S. and Kulkarni, S. (2009), 'Risk-Based Neuro-Grid Architecture for Multimodal Biometrics', *IEEE's International Conference on Systems, Computing Sciences and Software Engineering (CISSE-SCSS 09)*, 4-12 December, University of Bridgeport, USA, Vol. 2, Springer-Verlag, New Jersey.

[21] R. Tronci, G. Giacinto and F. Roli, "Selection of experts for the design of multiple biometric systems", *Lecture Notes in Computer Science*, 4571, pp 795-809 (2007).

[22] Center for Biometrics & Security Research: cbsr.ia.ac.cn/databases.asp

[23] Yale Face Database: cvc.yale.edu/projects/yalefaces/yalefaces.html

[24] A. Ross and R. Govindarajan, "Feature level fusion using hand and face biometrics", *Proceedings of the SPIE Conference on Biometric Technology for Human Identification II*, 5779, pp 196–204, 2005.

[25] L. Wang, H. Ning, T. Tan and W. Hu, "Fusion of static and dynamic body biometrics for gait recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, 14(2), pp 149-158, 2004.

[26] M. Faundez-Zanuy, "2004, Data fusion in biometrics", *IEEE Aerospace and Electronic Systems Magazine*, 20(1), pp 34-38, 2005..

[27] M. Indovina, U. Uludag, R. Snelick, A. Mink and A. Jain, "Multimodal biometric authentication methods: a COTS approach", *Proceeding of the MMUA 2003, Workshop on Multimodal User Authentication*, Santa Barbara, California, pp 99-106, 2003.

[28] F. Roll, K. Josef, F. Giorgio, and M. Daniele, "An Experimental Comparison of Classifier Fusion Rules for Multimodal Personal Identity Verification Systems", *Proceedings of Third International Workshop*, Cagliari, Italy, 2002.

[29] Y. Wang, T. Tan, and A. Jain, "Combining Face and Iris Biometrics for Identity Verification", *Proceedings of Fourth International Conference on Audio and Video-based Biometric Person Authentication (AVBPA'03)*, Guiford, U.K., 2003.

[30] A. George, "Bizarre Approaches For Multimodal Biometrics, International", *Journal of Computer Science and Network Security*, Vol.8, No.7, pp.64-69, 2008

[31] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain, "Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 27, No. 3, pp. 450-455, 2005.

[32] K. Czajkowski, S. Fitzgerald, I. Foster and C. Kesselman, "Grid Information Services for Distributed Resource Sharing", *Proceedings of 10th IEEE International Symposium on High Performance Distributed Computing*, pp. 181-184. IEEE Press, New York 2001.

[33] M. Atkinson, A. Chervenak, P. Kunszt, I. Narang, N. Paton, D. Pearson, A. Shoshani, and P. Watson, "Data access, integration, and management", In *The Grid: Blueprint for a New Computing Infrastructure*, 2nd Ed., I. Foster and C. Kesselman, Eds. Morgan Kaufmann, San Francisco, CA, 2004.

[34] R. Butler, V. Welch, D. Engert, I. Foster, S. Tuecke, J. Volmer, and C. Kesselman, "A National-scale Authentication Infrastructure", *IEEE Computer*, Vol. 33, No. 12, pp. 60–66, 2000.

[35] K. Keahey, I. Foster, T. Freeman, and X. Zhang, "Virtual workspaces: Achieving quality of service and quality of life in the grid", *Scientific Programming*, Vol. 13, No. 4, pp. 265-275. 2005.

[36] S.A. Mokhov, "Choosing Best Algorithm Combinations for Speech Processing Tasks in Machine Learning Using MARF", *Advances in Artificial Intelligence*, In LNAI 5032, S. Bergler, Ed., pp. 216-221, Springer-Verlag, Berlin Heidelberg, 2008.