Risk-Based Neuro-Grid Architecture for Multimodal Biometrics

Sitalakshmi Venkataraman[1], Siddhivinayak Kulkarni[2]

Academic Research Members of Internet Commerce and Security Laboratory,
Graduate School of Information Technology and Mathematical Sciences,
University of Ballarat, PO Box 663, Ballarat, VIC 3353, Australia

[1] s.venkatraman@ballarat.edu.au

[2] s.kulkarni@ballarat.edu.au

Abstract—Recent research indicates that multimodal biometrics is the way forward for a highly reliable adoption of biometric identification systems in various applications, such as banks, businesses, government and even home environments. However, such systems would require large distributed datasets with multiple computational realms spanning organisational boundaries and individual privacies.

In this paper, we propose a novel approach and architecture for multimodal biometrics that leverages the emerging grid information services and harnesses the capabilities of neural network as well. We describe how such a neuro-grid architecture is modelled with the prime objective of overcoming the barriers of biometric risks and privacy issues through flexible and adaptable multimodal biometric fusion schemes. On one hand, the model uses grid services to promote and simplify the shared and distributed resource management of multimodal biometrics, and on the other hand, it adopts a feed-forward neural network to provide reliability and risk-based flexibility in feature extraction and multimodal fusion, that are warranted for different real-life applications. With individual autonomy, scalability, risk-based deployment and interoperability serving the backbone of the neuro-grid information service, our novel architecture would deliver seamless and robust access to geographically distributed biometric data centres that cater to the current and future diverse multimodal requirements of various day-to-day biometric transactions.

Keywords: Biometric Technologies, Transaction Risks, Multimodal Biometrics, Grid Services, Data Grids, Neural Networks

I. Introduction

With the escalating increase in digital impersonation being witnessed today, biometric identification becomes a highly secure personal verification solution to the problem of identity theft [1]. Since a biometric trait of a person (e.g. fingerprint, hand geometry, signature, retina, voice, gait, etc.) has a strong relationship to his or her identity, it confirms the person making a transaction leading to satisfying the authentication, authorisation and non-repudiation objectives of information security. Hence, biometric verification is being increasingly considered in a wide variety of everyday applications in business, service and even home and schools [2]. However, in order for biometrics to be successful, such advanced systems should also be able to deal with privacy concerns, performance problems and multiple trait issues [3].

Biometric technology needs to address the following critical problems:

i) Permanence – Biometric data may be required to be revoked and reissued due to security breach or changes in the person's features due to factors such as aging or deformity [4].
ii) Multiple Traits - Different biometric technologies are at different stages of maturity [5] and there is no single trait that could become the standard for all applications. Multiple biometric enrolments for different situations pose a major inconvenience to the users [6].
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 [7].

To solve the above said problems, multimodal biometric systems, which consolidate information from a person's multiple biometric samples (e.g. fingerprints of the same finger), multiple instances (e.g. fingerprints of different fingers) and multiple traits (e.g. fingerprint and iris scan), are becoming popular While there is a strong motivation for multimodal biometrics, such systems would require advanced biometric technology interfaces and policy framework that caters to performance, security and privacy issues for a successful adoption in everyday life [8]. 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).

Grid information services, which provide scalability, security and high-performance features to the distributed and heterogeneous resources [9], offer promise to overcome the aforesaid limitations of the current unimodal and multimodal biometric systems. Hence, this paper aims to present a biometric grid architecture that could launch an adaptive multimodal biometrics effectively through the use of neural networks for addressing security and privacy risks in real-life applications. Such a neuro-grid architecture could compensate the weakness of any biometric classifier by other stronger biometric classifiers through the distributed grid service to achieve accuracy and reliability of multimodalities in a collaborative and flexible manner. In this way, biometric systems could be tuned to meet the changing business and user requirements. In other words, this paper explores the

T. Sobh, K. Elleithy (eds.), *Innovations in Computing Sciences and Software Engineering*,
DOI 10.1007/978-90-481-9112-3_9, © Springer Science+Business Media B.V. 2010

integration of two concepts, namely neural networks and grid computing for an improved multimodal biometric system of the future.

The rest of the paper is organized as follows. Section 2 presents a brief overview of the essential features of Grid Information Services required for biometric transaction processing. Section 3 describes how the complex fusion scheme of multimodal biometrics could be enabled through neural network fusion technique that uses a risk-based classification of biometric transactions. In Section 4, we propose risk-based neuro-grid architecture for multimodal biometrics using a feed-forward neural network. Finally, in Section 5, we provide conclusions and directions of future work.

II. Grid Information Services in Biometrics

A grid is a collection of distributed services launched in a portal through which users or business applications interact for their information processing services [9]. In this section, we provide an overview of typical grid information services (Fig. 1) that could cater to the needs of various biometric users or applications. As depicted in Fig. 1, we describe below, the main basic and advanced functions of grid information services that are highly useful for processing biometric transactions:

i) Basic functions – The basic features of discovery and brokering, data sharing, monitoring and policy controlling are essential for processing multiple biometric classifiers in a distributed grid environment.

ii) Advanced functions – The advanced features associated with security and resource management capabilities of grid information services play a crucial role in achieving accuracy and reliability of biometric transactions in a distributed grid environment.

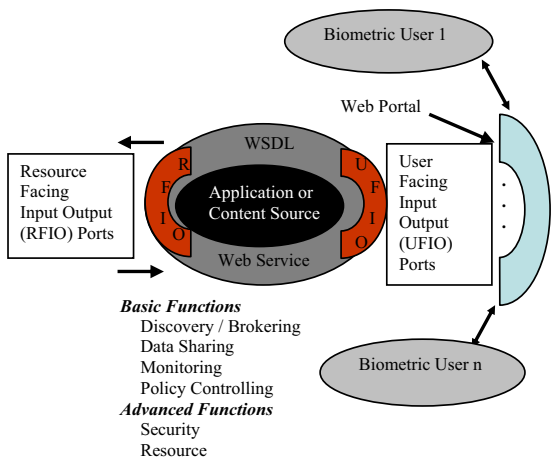

Fig. 1. Typical grid information services for biometric users

Discovery and Brokering: This functionality helps in the discovery of biometric resources and brokering of different biometric traits 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 so that the matching measures are computed successfully 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 inherent noise.

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 authentication, authorisation and accounting mechanisms required for processing biometric data. The capability of grid information services with dynamic instantiation of new security features and services becomes an advanced feature for biometric applications.

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

III. Multimodal Biometric Fusion using Neural Networks

Recent research studies indicate that privacy and security risks are the prime factors for society to be slow in embracing biometrics [7]. Hence, in order to reap the benefits of this emerging technology as a highly secure personal verification solution against information security threats, we need to identify and address the possible privacy and security risks that biometric transactions could pose within commercial as well as non-commercial scenarios. More importantly, a classification of these transactions based on the risk levels, such as , 'Basic', 'Intermediate' and 'Advanced' [10], would aid in providing the necessary flexibility and adaptability that Grid information services could leverage upon while matching with each user's multimodal biometric preferences.

A. Complexities of Multimodal Biometric Fusion

In multimodal biometrics of a multiple classifier system, the fusion module chosen by the grid information service is required to be based on a few associated criteria so that the grid-based architecture could match the user-centric preferences of the biometric traits with the business transaction requirements towards addressing the privacy and security risk issues. We identify the following criteria with

which the grid information service could be modeled to adopt the most appropriate fusion algorithm:

i) Level of system balance – The level of accuracy of multiple biometric classifiers could vary among different traits [11]. If all the classifiers to be included in the fusion module are of high level of accuracy, then the level of system balance is set to be high. Hence, the level of system balance could be determined based on the classifier accuracy levels and their differences.

ii) Degree of complexity – This is determined based on the computational complexity of the fusion algorithm in the matching process of multiple biometrics. There are simple techniques such as the sum rule, decision tree, plain averaging formula, etc. [12]. Some of the highly complex techniques adopt trained rule base classifiers that make use of Support Vector Machines (SVM), neural networks, Bayes / radial basis network, etc [13].

iii) Level of privacy / security risk – Biometric transactions could be classified based on the risk levels associated, such as, basic, medium or advanced. This gives an indication to the grid information service the type of biometric classifiers to be used for processing the transaction. A holistic analysis of risk levels for biometric authentication would be based on technology, privacy, safety, performance and security issues that surround biometrics in an integrated manner [14].

Many research studies have demonstrated that fusion is more effective in the identification of an individual than single classifiers [15]. However, if unbalanced classifiers are combined, a highly complex fusion technique may take more time to optimise and would eventually degrade the system performance. Hence, for many simple transactions that fall under basic risk level, the grid information system could make use of unimodal biometrics. On the other hand, certain financial transactions, even though assigned basic privacy risk level, may require classifiers with high system balance as preferred by the user and may involve complex fusion techniques. In open-population applications such as airports, simple sum fusion could be more effective, whereas in closed-population applications such as office, user weighting fusion methods could be more effective. Hence, the above three inter-related criteria could be incorporated as privacy policy rules for the grid information system to be flexible in adopting the appropriate fusion technique for biometric authentication based on the transaction scenario. To achieve this, we propose the use of neural networks for the feature extraction step and fusion technique adoption step that are required for processing a biometric identification transaction. These steps are briefly summarized next.

B. Neural Network-Based Feature Extraction

Overall, privacy and security risks could be identified with biometrics during the very first interaction with the user, namely, the enrolment process, when biometric data is collected and stored as signatures or normalised as templates. Neural network models that have been successfully adopted in image analysis and pattern recognition [16] [17], could be considered for biometric applications. We propose a Multi Layer Perceptron (MLP) neural network that learns the same biometric trait at the input and output neurons and provides a characteristic through its hidden layer as a feature vector. The main advantages of using a MLP neural network are adaptability, noise tolerance and collective computability [18], which are the main features required for multimodal biometrics. The number of hidden layers may vary depending upon the characteristics of the feature vectors and the synaptic weights are determined to minimize error [19].

We provide an example MLP as a fingerprint feature extractor in Fig. 2. Here, the features are extracted from fingerprint images which are usually texture patterns. The output obtained from the hidden layer of MLP will be taken as fingerprint feature vectors. In general, the feature vector obtained (hidden layer output) can be considered as a two dimensional block of hidden node outputs, each hidden node having N_i outputs so that the total dimension of a feature is N_h by N_i, where N_h is the number of hidden nodes in the hidden layer and N_i is the number of inputs applied to the MLP. As shown in Fig. 2, the example MLP given here learns the same patterns with a single hidden layer in the feed-forward neural network that provides the biometric feature vector. The MLP with the same texture patterns at input and output could be trained using a supervised learning algorithm. A compelling advantage of this technique is that the training is quite fast and provides consistency between the extracted features of the same class [20]. This will help in the classification of extracted features accurately and to adopt appropriate fusion algorithm in the verification and application stages based on the risks associated with the biometric transaction.

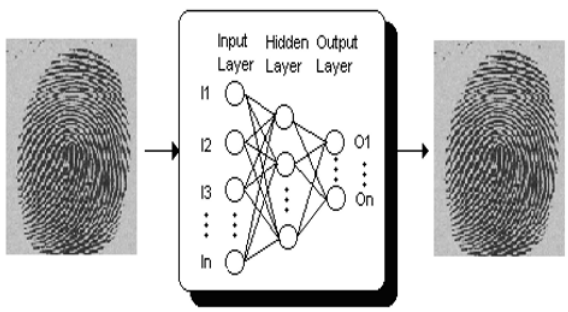

Fig. 2. Multi Layer Perceptron (MLP) as feature extractor

C. Neural Network-Based Multimodal Fusion Scheme

We propose a fusion scheme that is based on N-layer feed-forward neural network. The number of inputs to the neural network is equivalent to the number of biometric techniques used and the output of the neural network is called the Fusion Factor. The neural network decides the final fusion factor for the combination of the N different biometric classifiers, where MS_i denotes the matching score of classifier i. Fig. 3 depicts a typical N-layer feed-forward neuro-based multimodal fusion approach.

We illustrate a 2-layer feed-forward neural network with two traits, namely fingerprint and iris for training bimodal biometric fusion technique in Table 1. If the matching score (MS) for the first classifier is MS_1 and the matching score for the second classifier is MS_2 these two scores could be applied to neural network as input and the resulting fusion factor is indicated by F_1 in the first iteration. As illustrated in Table 1, let the matching scores be 0.7 and 0.9 for two different biometric traits (Case-I), and 0.8 and 0.7 (Case-II) for another instance of these traits. The neural network determines the fusion factor for Case-I and Case-II as A and B respectively, which are compared. For the illustrated dataset, we would expect the fusion factor B to be less than A and the neural network could discard B and consider another bimodal dataset for the next training iteration. This way, the feed-forward neural network gets trained with the prime objective of minimising False Acceptance Rate (FAR) and False Rejection Rate (FRR). Through the generation of fusion factors, the expected threshold values of the three criteria, namely, level of system balance, degree of complexity and risk levels are determined for risk-based biometric transaction processing.

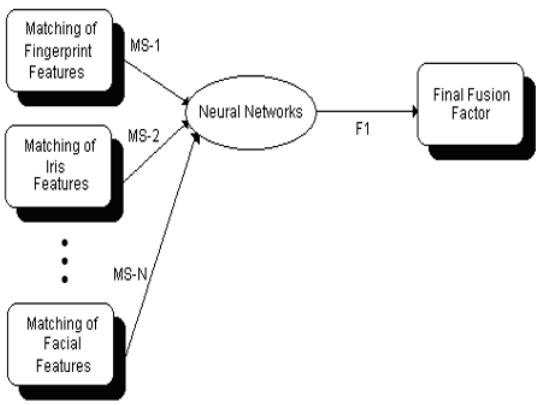

Fig. 3. Feed-forward neuro-based multimodal fusion technique

Table 1: Neuro-based training for multimodal fusion technique

Biometric Cases	Matching Score for Fingerprint Technique (MS1)	Matching Score for Iris Technique (MS2)	Fusion Factor (F1)
Case-I	0.7	0.9	A
Case-II	0.8	0.7	B (A>B)

IV. Risk-Based Biometric Neuro-Grid Architecture

We propose a grid architecture that uses a feed-forward neural network for incorporating risk-based multimodal biometric fusion schemes. 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. We present an overview of the biometric neuro-grid architecture in Fig. 4, which shows the major components involved. We describe briefly the components that constitute our risk-based biometric neuro-grid architecture from the top layer to the bottom layer, with inputs of risk parameters and biometric fusion parameters that would get processed from one layer to the other using a feed-forward neural network.

A. Biometric Client Application Layer

This 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 biometric trait preferences for different applications based on the risk levels associated with those biometric-enabled transactions. The portal uses such parameters to associate biometric metadata with datasets that are utilized in the next layer to determine their resource location for data retrieval and publication.

B. High-level and Multimodal Biometric Services

In this second layer of the grid architecture, the high-level grid service provides 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 [21]. 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 feed-forward MLP 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 neuro-based 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. A shared data access could be incorporated for integrating shared authorisation service for both group-based and individual access to datasets through GridFT [22]. Apart from enforcing data encryption through GSI, reliability could also be enhanced through the monitoring infrastructure through the use of Globus Toolkit's grid information services [23]. The Grid Resource Allocation and Management (GRAM) sub-

component provides the necessary service to communicate between the multimodal biometric recognition module provided by the feed-forward MLP and the grid services modules to access and process biometric data.

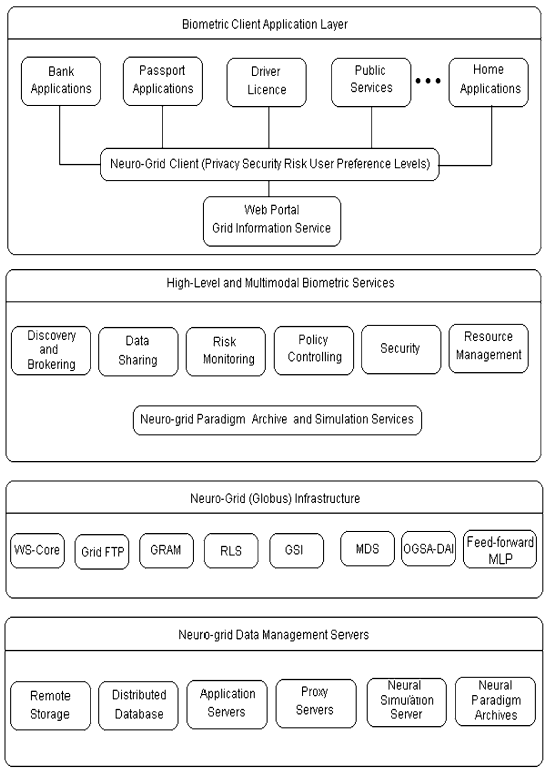

Fig. 4. Neuro-grid architecture for multimodal biometrics

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 MLP as biometric feature extractor and the feed-forward neurons for the multimodal fusion adoption scheme. The fusion adoption scheme determines the best of 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 [24]. The training paradigms in this context are preserved as archives of the machine learning process for future references. In summary, this layer provides all the necessary resources for executing biometric transactions and to provide computational power to users who make use of the Web grid services at the client-end of the various biometric applications.

V. Conclusions and Future Work

In this paper, we have presented a novel risk-based grid architecture that uses feed-forward neural network for multimodal biometric fusion. The motivation of the proposed architecture is to address the risk-based adoption issues surrounding biometrics. While multimodal biometrics are capable of overcoming the limitations posed by unimodal biometrics, such as, permanence, multiple traits and individual privacy, its success in adoption require information sharing among large, heterogeneous and distributed multimodal data centres. This warrants features such as, advanced biometric data access, sophisticated multimodal fusion algorithms and more importantly, an adaptive privacy policy framework, and these form the main backbone of our proposed risk-based neuro-grid architecture for multimodal biometrics.

Our proposed neuro-grid architecture takes advantage of the recent evolution of OGSA's GSI3 that provides an improved security model, network services and other information services through a Web portal. It provides the optimal setting for the discovery, data sharing, monitoring and managing multimodal biometric resources that are diverse, large, dynamic and distributed among organisations. Further, by combining with neural network capabilities, the proposed architecture caters to three parameters such as multimodal biometric system balance, degree of complexity of fusion schemes and privacy / security risk levels that feed into the training and adaptive rules of the policy framework. Since such a feed-forward neural network combines the information from different biometric modalities as preferred by the individual user for specific biometric transactions and checks the compatibility within the policy framework of each application environment, it is aimed at providing the necessary risk-based decisions for an improved diffusion of multimodal biometrics.

Looking forward, there is much to be gained from neural network and grid computing researchers, and this paper provides motivation for such inter-disciplinary research with applications in multimodal biometrics. With the increased interest in neural network based multimodal biometric fusion, an interesting topic for future research entails investigation of different number of hidden layers in the feed-forward neural network that could impact on the performance and accuracy of fusion schemes. Another topic of future research is to explore collaborative data sharing of multimodal biometrics among different organisations to take advantage of the proposed neuro-grid information service.

REFERENCES

[1] R. Condon, "New Biometrics See Right through You", *Information Security*, Vol. 4, No. 1, pp. 24-26, 2007.

[2] 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.

[3] R. Ryan, "How to Successfully Design and Deploy Biometrics to Protect Identity and Overcome Privacy Concerns", *The Winter 2007 Biometrics Summit*, Miami, Florida, 2007.

[4] 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 Biometrics,* Vol. 14, No. 1, pp. 4-20, 2004.

[5] K. Chang, K. W. Bowyer, S. Sarkar and B. Victor, "Comparison and Combination of Ear and Face Images in Appearance-Based Biometrics", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 25, No. 9, pp. 1160-1165, 2003.

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

[7] International Biometric Group, "Biometrics Market and Industry Report 2007-2012", *Biometrics Report and Research,* http://www.biometricgroup.com, 2007.

[8] 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.

[9] 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.

[10] 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.

[11] A. Teoh, S. Samad, and A. Hussain, "Nearest Neighbourhood Classifiers in a Bimodal Biometric Verification System Fusion Decision Scheme", *Journal of Research and Practice in Information Technology*, Vol. 36, No. 1, pp. 47-62, 2004.

[12] 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.

[13] 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.

[14] A. Bromme, "A Risk Analysis Approach for Biometric Authentication Technology", *International Journal of Network Security*, Vol. 2, No. 1, pp. 52–63, 2006.

[15] 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.

[16] M. Egmont-Petersen, D. De Ridder, H. Handels, "Image Processing with Neural Networks - a review". *Pattern Recognition* Vol. 35, No. 10: 2279–2301, 2002.

[17] B.B. Nasution and A.I. Khan, "A Hierarchical Graph Neuron Scheme for Real-Time Pattern Recognition", *IEEE Transactions on Neural Networks*, Vol 19, No. 2, pp. 212-229, 2008.

[18] B. Widrow, and R. Winter, "Neural Nets for Adaptive Filtering and Adaptive Pattern Recognition", *IEEE Computer*, Vol. 21, No. 3, pp. 25-39, 1988.

[19] D. Mandic, & J. Chambers, *Recurrent Neural Networks for Prediction: Architectures, Learning algorithms and Stability*. Wiley, 2001.

[20] S. Kulkarni, and B. Verma, "An Autoassociator for Automatic Texture Feature Extraction", *Proceedings of 4th International Conference on Computational Intelligence and Multimedia Applications (ICCIMA '01)*, pp. 328-332, Yokosuka, Japan, 2001.

[21] 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.

[22] 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.

[23] 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.

[24] 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