Neural networks for Multibiometrics – Review on Issues, Applications, Challenges and Research Areas

B.Revathi @ Ponmozh*, Dr. G.F.Sudha**
*Research Scholar, Pondicherry Engineering College, Puducherry.
**Associate Professor, Pondicherry Engineering College, Puducherry.

Abstract
Recent Advances in the field of Information Technology makes Information Security an inseparable part of it. In order to deal with security, Authentication plays an important role. This paper presents a review on the biometric authentication techniques and some future possibilities in this field. Biometric authentication systems makes use neural networks for the training and verification phase. The fusion of multiple biometrics helps to minimize the system error rates. Fusion methods include processing biometric modalities sequentially until an acceptable match is obtained. This paper is an overview of Neural networks for multibiometrics, challenges in the progress of multibiometrics using neural networks, the main research areas and its applications to develop the security system for high security areas.

Keywords: Unimodal, Multibiometrics, ANN

1. INTRODUCTION

Information security deals with the assurance of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security. But system based on biometric has evolved to support some aspects of information security. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security. Biometric authentication has grown in popularity as a way to provide personal identification. Person’s identification is crucially significant in many applications and the hike in credit card fraud and identity theft in recent years indicates that this is an issue of major concern in wider society. Individual passwords, pin identification or even token based arrangement all have deficiencies that restrict their applicability in a widely-networked society. Biometric is used to identify the identity of an input sample when compared to a template, used in cases to identify specific people by certain characteristics. Possession based: using one specific "token" such as a security tag or a card and knowledge-based: the use of a code or password. Standard validation systems often use multiple inputs of samples for sufficient validation, such as particular characteristics of the sample. This intends to enhance security as multiple different samples are required such as security tags and codes and sample dimensions. So, the advantage claimed by biometric authentication is that they can establish an unbreakable one-to-one correspondence between an individual and a piece of data.

Biometric systems based on single source of information are called unimodal systems. Although some unimodal systems [2] have got considerable improvement in reliability and accuracy, they often suffer from enrollment problems due to non-universal biometrics traits, susceptibility to biometrics spoofing or insufficient accuracy caused by noisy data [3]. Hence, single biometric may not be able to achieve the desired performance requirement in real world applications. One of the methods to overcome these problems is to make use of multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision. Studies have demonstrated that multimodal biometric systems can achieve better performance compared with unimodal systems.

This paper presents the review of neural networks for multibiometrics. This includes applications, challenges and areas of research in multimodal biometrics. The different fusion techniques of multimodal biometrics have been discussed. The paper is organized as follows. A detailed literature has been presented in Section 2 followed by Multialgorithm and multi sample approach in Section 3 whereas need of multibiometrics and details of Multibiometrics are illustrated in Section 4 and Section 5 respectively. Artificial Neural Networks along with its architecture is discussed in Section 6. Applications of Neural Networks in Multibiometrics are illustrated in Section 7, whereas Challenges and research areas are given in Section 8. Summary and Conclusions are presented in the last section of the paper.

B.Revathi, Dr. G.F.Sudha
2. LITERATURE SURVEY

Combining several systems has been investigated in pattern recognition [1] in general; in applications related to audiovisual speech processing [3]; in speech recognition—examples of methods are multi-band, multi-stream, front-end multi-feature approaches and the union model [9]; in the form of ensemble [10]; in audio-visual person authentication; and, in multi-biometrics [12], [13], [14], [15], [16] (and references herein), among others. In fact, one of the earliest works addressing multimodal biometric fusion was reported in 1978 [17]. Therefore, biometric fusion has a history of 30 years. Recent advances in multi-biometrics have been focusing on quality-based fusion, e.g., [18], [19], [20], [21], [22], where the quality associated with the template as well as the query biometric sample are taken into account in decision level fusion. For this purpose, a plethora of quality measures have recently been proposed in the literature for various biometric modalities, e.g., fingerprint [23], [24], iris [25], face [26], speech [27], signature [28], and classifier-dependent measure [29]. The proposed quality measures, in general, aim to quantify the degree of excellence of biometric samples of higher quality are given more important consideration, i.e., higher weights, in order to compute the final combined score. There are two ways quality measures can be incorporated into a fusion classifier, depending on their role, i.e., either as a control parameter or as evidence. In their primary role, quality measures are used to modify the way a fusion classifier is trained or tested, as suggested in the Bayesian based classifier called “expert conciliation” [18], reduced polynomial classifier [31], quality-controlled support vector machines [19], and quality-based fixed rule fusion [32]. In their secondary role, quality measures are often concatenated with the expert outputs to be fed to a fusion classifier, as found in logistic regression [20] and the mixture of Gaussians Bayesian classifier [21].

Other notable work includes the use of Bayesian network to gauge the complex relationship between expert outputs and quality measures, e.g., Maurer and Baker’s Bayesiannetwork [33] and Pohet al.’s quality state-dependent fusion [34]. The work in [34] takes into account an array of quality measures rather than representing quality as a scalar. By means of grouping the multi-faceted quality measures, a fusion strategy can then be devised for each cluster of quality values. Other suggestions include the use of quality measures to improve biometric device interoperability [35], [36]. Such an approach is commonly used in speaker verification [37] where different strategies are used for different microphone types.

Last but not least, another promising direction in fusion is to consider the reliability estimate of each biometric modality. In [38], the estimated reliability for each biometric modality was used for combining symbolic-level decisions, whereas in [39], [40], [41], [30], score-level fusion was considered. However, in [39], [40], [41], the term “failure prediction” was used instead. Such information, derived solely from the expert outputs (instead of quality measures), has been demonstrated to be effective for single biometric modalities [39], fusion across sensors for a single biometric modality [40], and across different machine learning techniques [41]. In [30], the notion of reliability was captured by margin, a concept used in large-margin classifiers [42]. Exactly how the reliability is defined and estimated for each modality, and how it can be effectively used in fusion, are still open research issues.

3. MULTI ALGORITHM AND MULTI SAMPLE APPROACH

Multi algorithm approach employs a single biometric sample acquired from a single sensor. (Figure 1) Two or more different algorithms process this acquired sample. The individual results are combined to obtain an overall recognition result. This approach is attractive, both from an application and research point of view because of use of single sensor reducing data acquisition cost. The 2002 Face Recognition Vendor Test has shown increased performance in 2D face recognition by combining the results of different commercial recognition systems [4]. Gokberk et al. [5] have combined multiple algorithms for 3D face recognition. Xu et al. [6] have also combined different algorithmic approaches for 3D face recognition.

Multi sample or multi instance algorithms use multiple samples of the same biometric. The same algorithm processes each of the samples and the individual results are fused to obtain an overall recognition result. In comparison to the multi algorithm approach, multi sample has an advantage that using multiple samples may overcome poor performance due to one sample that has unfortunate properties. Acquiring multiple samples requires either multiple copies of the sensor or the user availability for a longer period of time. Compared to multi algorithm, multi sample seems to require either higher expense for sensors, greater cooperation from the user, or a combination of both. For example, Chang et al. [7] used a multi-sample approach with 2D face images as a baseline...
against which to compare the performance of multi-sample 2D + 3D face.

4. NEED OF MULTIBIOMETRICS

Most of the biometric systems deployed in real world applications are unimodal which rely on the evidence of single source of information for authentication (e.g. fingerprint, face, voice etc.). These systems are vulnerable to variety of problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing.

Figure 1: Fusion in multibiometric system

It leads to considerably high false acceptance rate (FAR) and false rejection rate (FRR), limited discrimination capability, upper bound in performance and lack of permanence [8]. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. These systems allow the integration of two or more types of biometric systems known as multimodal biometric systems. These systems are more reliable due to the presence of multiple, independent biometrics. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge – response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a ‘live’ user is indeed present at the point of data acquisition.

5. MULTIBIOMETRICS

The term “multimodal” is used to combine two or more different biometric sources of a person (like face and fingerprint) sensed by different sensors. Two different properties (like infrared and reflected light of the same biometric source, 3D shape and reflected light of the same source sensed by the same sensor) of the same biometric can also be combined. Inorthogonal multimodal biometrics, different biometrics (like face and fingerprint) are involved with little or no interaction between the individual biometric whereas independent multimodal biometrics processes individual biometric independently. Orthogonal biometrics are processed independently by necessity but when the biometric source is the same and different properties are sensed, then the processing may be independent, but there is at least the potential for gains in performance through collaborative processing. In collaborativemultimodal biometrics the processing of one biometric is influenced by the result of another biometric.

A generic biometric system has sensor module to capture the trait, feature extraction module to process the data to extract a feature set that yields compact representation of the trait, classifier module to compare the extracted feature set with reference database to generate matching scores and decision module to determine an identity or validate a claimed identity. In multimodal biometric system information reconciliation can occur at the data or feature level, at the match score level generated by multiple classifiers pertaining to different modalities and at the decision level. Biometric systems that integrate information at an early stage of processing are believed to be more effective than those which perform integration at a later stage. Since the feature set contains more information about the input biometric data than the matching score or the output decision of a matcher, fusion at the feature level is expected to provide better recognition results. However, fusion at this level is difficult to achieve in practice because the feature sets of the various modalities may not be compatible and most of the commercial biometric systems do not provide access to the feature sets which they use. Fusion at the decision level is considered to be rigid due to the availability of limited information. Thus, fusion at the match score level is usually preferred, as it is relatively easy to access and combine the scores presented by the different modalities [2].

Rukhin and Malioutov [10] proposed fusion based on a minimum distance method for combining rankings from several biometric algorithms. Fusion methods were compared by Kittler et al. [11], Verlinden et al. [12] and Fierrez Aguilar et al. [13]. Kittler found that the sum rule outperformed many
other methods, while Fierrez-Aguilar et al. [13, 14] and Gutschovenand Verlinde [15] designed learning based strategies using support vector machines. Researchers have also investigated the use of quality metrics to further improve the performance [16, 14, 17–21]. Many of these techniques require the scores for different modalities (or classifiers) to be normalized before being fused and develop weights for combining normalized scores. Normalization and quality weighting schemes involve assumptions that limit the applicability of the technique. In [22], Bayesian belief network (BBN) based architecture for biometric fusion applications is proposed. Bayesian networks provide unified probabilistic framework for optimal information fusion. Although Bayesian methods have been used in biometrics [16, 23–25], the power and flexibility of the BBN has not been fully exploited.

Brunelli et al. [26] used the face and voice traits of an individual for identification. A Hyper Bf network is used to combine the normalized scores of five different classifiers operating on the voice and face feature sets. Bigun et al. [16] developed a statistical framework based on Bayesian statistics to integrate the speech (text dependent) and face data of a user [27]. The estimated biases of each classifier are taken into account during the fusion process. Hongand Jain associate different confidence measures with the individual matchers when integrating the face and fingerprint traits of a user [28]. They also suggest an indexing mechanism wherein face information is used to retrieve a set of possible identities and the fingerprint information is then used to select a single identity. A commercial product called BioID [29] uses the voice, lip motion and face features of a user to verify the identity. Aloysius George used Linear Discriminant analysis (LDA) for face recognition and Directional filterbank (DFB) for fingerprint matching. Based on experimental results, the proposed system reduces FAR down to 0.0000121%, which overcomes the limitation of single biometric system and proves stable personal verification in real-time [30].

6. ARTIFICIAL NEURAL NETWORK

Artificial Neural Network (ANNs) has a large appeal to many AI researchers. A neural network can be defined as a model of reasoning based on the human brain. The brain consists of a closely interconnected set of nerve cells or basic information-preprocessing units, called neurons. The human brain incorporates nearly 10 billion neurons and 60 trillion connections, synapses between them [Shepherd, 1990]. By using multiple neurons simultaneously, the brain can perform its functions much faster than the fastest computers in existence today [Negnevitsky, 2002].

A multilayer perceptron is a feed-forward neural network with one or more hidden layers. Typically, the network consists of an input layer of source neurons that at least one hidden layer of neurons and an output layer of neurons (Figure 2). The input signals are propagated in a forward direction on a layer-by-layer basis. The backpropagation algorithm is perhaps the most popular and widely used neural paradigm.

![Feed-forward Neural Network](image)

**Figure 2: Feed-forward Neural Network**

It is based on the generalized delta rule proposed by research group in 1985 headed by Dave Rumelhart based at Stanford University, California, USA.

Before the network can be used, it requires target patterns or signals as a supervised learning algorithm. Training patterns are obtained from the samples of the types of inputs to be given to the backpropagation neural network and their targets are identified by the researchers. The objective of the algorithm is to find the next value of adaptation weight which is also known the Generalized Delta Rule (G.D.R).

The hidden layer weights are adjusted using the errors from the subsequent layer. Thus, the errors computed at the output layer are used to adjust the weight between the last hidden and the output layer. Likewise, an error value computed from the last hidden layer outputs are used to adjust the weight in the next to the last hidden layer and so on until the weight connections to the first hidden layer are adjusted. In this way, errors are propagated backwards layer by layer with corrections being made to the corresponding layer weights in an iterative manner. The process is repeated a number of times for each pattern in the training set until the total error converges to a minimum or until some limit is reached in the number of training iterations completed [Patterson, 1999].

6.2 The Activation Function
The activation function has the characteristics of continuity, differentiability and non-decreasing uniformity. There is several activation functions used in neural network. There is several activation functions used in the neural network. Binary sigmoid and bipolar sigmoid are generally used in the neural network training. The binary sigmoid which has a normalized range within 0 and 1 and bipolar sigmoid is normalized within -1 to +1 are used in backpropagation training.

7. APPLICATIONS OF NEURAL NETWORKS IN MULTIBIOMETRICS

The neural network has the ability of storing the information of the continuous quantity. The detailinformation of the continuous quantity can be calculated from the whole network, and also determine the wholenetwork. The paper by Garriset al. provides an overview of the NN-based approaches to optical character recognition (OCR). They also provide an end-to-end OCR recognition system based on an enhanced multilayer perceptron (MLP) classifier. The paper by Phillips presents a face identification algorithm that automatically processes an unknown image by locating and identifying the face. His algorithm is based on designing anet of matching pursuit filters optimized for face detection and identification. For identification, the filters find features that differentiate among faces, whereas, for detection, the filters encode the similarities among faces. This algorithm has been evaluated on three sets of images. The first set was images from the FERET data base (a well-known benchmarking dataset for face recognition). The second set was infrared and visible images of the same people. This demonstration was done to compare performance on infrared and visible images individually, and on fusing the results from both modalities. The third set was mugshot data from a law enforcement application.

The defense and intelligence communities require automated methods capable of rapidly determining an individual’s true identity as well as any previously used identities and past activities, over a geospatial continuum from set of acquired data. A homeland security and law enforcement community require technologies to secure the borders and to identify criminals in the civilian law enforcement environment. Key applications include border management, interface for criminal and civil applications, and first responder verification.

Enterprise solutions require the oversight of people, processes and technologies. Network infrastructure has become essential to functions of business, government, and web-based business models. Consequently securing access to these systems and ensuring one’s identity is essential. Personal information and business transactions require fraud prevention solutions that increase security and are cost effective and user friendly. Key application areas include customer verification at physical point of sale, online customer verification etc.

Designing biometric sensors, which automatically recognize the operating environment (outdoor / indoor / lighting etc) and communicate with other system components to automatically adjust settings to deliver optimal data, is also the challenging area. The sensors should be fast in collecting quality images from a distance and should have low cost with no failures to enroll [IJBB5].

The multimodal biometric systems can be improved by enhancing matching algorithms, integration of multiple sensors, analysis of the scalability of biometric systems, followed by research on scalability improvements and quality measures to assist decision making in matching process. Open standards for biometric data interchange formats, file formats, applications interfaces, implementation agreements, testing methodology, adoption of standards-based solutions, guidelines for auditing biometric systems and records and framework for integration of privacy principles are the possible research areas in the field.

8. CHALLENGES AND RESEARCH AREAS

Architectures There is a huge space of different fusion architectures that has not been explored. The range of possible configurations encompassing serial, parallel and hybrid structures is immense. While the parallel fusion strategy is most commonly used in multimodal biometric fusion, there are additional advantages in exploring serial fusion, where the experts are considered one at a time. It offers the possibility of making reliable decisions with only a few experts, leaving only difficult problems to be handled by the remaining experts.

Fusion strategies An important consideration when adopting a fusion strategy is to consider the statistical dependency among the expert outputs. For instance, in intramodal fusion, several experts may rely on the same biometric sample and so higher dependency is expected among the expert outputs. On the other hand, in a multimodal setting, the pool of experts is likely to be statistically independent. In [20], three types of frameworks are proposed in order to solve a multimodal fusion problem involving intramodal experts.

The first framework simply assumes independence, in which case the fusion classifier reduces to a Naive Bayes one.
The second framework considers dependency of experts in an intramodal setting (allobserving the same biometric modality) whereas ignores the dependency at the multimodal setting, hence realizing a twostage fusion process. Finally, the third framework makes no assumption about the expert outputs.

Expert selection Expert selection can be cast as a featureselection problem, as illustrated in [48]. However, directly applying such technique to biometric authentication is difficult. In Section III, for instance, we have seen that the optimal set of experts found using a development population of users may not be the best for the target users. The phenomenon, knownas “Doddington’s menagerie”, relates to the fact that each expert is affected by the differences in the ability of the users’ biometric models to represent their respective identities.

These diverse abilities have been characterized in Doddingtonetal. [49] by associating different animal names with the users, such as sheep and goats. Thus, a much more robust criterion, taking into account of Doddington’s menagerie, must be considered in expert selection. Anotherissue is raised by the cost considerations. Concretely, both the operational cost and performance into a single criterion proves to be a difficult task. A special problem of expert selection, called dynamic expert selection arises naturally in the serial fusion architecture. In dynamic expert selection, a fusion classifier may decide which expert is most informative to query even before the data is acquired. In the recent Multimodal Biometric benchmark evaluation, organized by the Biosecure (EU-funded) project 2, dynamic fusion strategy proved to be very promising in achieving good performance while minimizing costs.

9. SUMMARY AND CONCLUSIONS

This paper presented the various issues related to multimodal biometric systems. By combining multiple sources of information, the improvement in the performance of biometric system is attained. Various fusion levels and scenarios of multimodal systems are discussed. Neural network solutions like Support vector machine (SVM) helps to get Fusion at the match score level that is the most popular due to the ease in accessing and consolidating matching scores. Template security is critical to the integrity of a biometric system. Fuzzy vault and Fuzzy extractor are provided as solution to template security. Performance gain is pronounced when uncorrelated traits are used in multimodal system. The challenges faced by multimodal biometric system and possible research areas are also discussed in the paper.

REFERENCES


[27] National Institute of Standards and Technology, “Nist speech quality assurance package 2.3 documentation.”


