American Journal of Intelligent Systems 2013, 3(3): 105-112
DOI: 10.5923/j.ajis.20130303.01

# Soft Computing in Biometrics: A Pragmatic Appraisal

**M. A. Jayaram[1], Hasan Fleyeh[2,*]**

[1]Department of Master of Computer Applications Siddaganga Institute of Technology, Tumkur, India
[2]Computer Engineering Department, School of Technology and Business Studies, Dalarna University, Sweden

**Abstract** The ever increasing spurt in digital crimes such as image manipulation, image tampering, signature forgery, image forgery, illegal transaction, etc. have hard pressed the demand to combat these forms of criminal activities. In this direction, biometrics - the computer-based validation of a persons' identity is becoming more and more essential particularly for high security systems. The essence of biometrics is the measurement of person's physiological or behavioral characteristics, it enables authentication of a person's identity. Biometric-based authentication is also becoming increasingly important in computer-based applications because the amount of sensitive data stored in such systems is growing. The new demands of biometric systems are robustness, high recognition rates, capability to handle imprecision, uncertainties of non-statistical kind and magnanimous flexibility. It is exactly here that, the role of soft computing techniques comes to play. The main aim of this write-up is to present a pragmatic view on applications of soft computing techniques in biometrics and to analyze its impact. It is found that soft computing has already made inroads in terms of individual methods or in combination. Applications of varieties of neural networks top the list followed by fuzzy logic and evolutionary algorithms. In a nutshell, the soft computing paradigms are used for biometric tasks such as feature extraction, dimensionality reduction, pattern identification, pattern mapping and the like.

**Keywords** Soft-computing, Biometrics, Soft-biometrics, Fuzzy Logic, Neural Networks, Evolutionary Algorithms, Hybrid Systems

## 1. Introduction

Biometrics (ancient Greek: *bios* meaning life, *metron* meaning measure) is a fusion of two domains of study and application. One dealing with biology and the other dealing with the process of devising schemes for the authentication of individuals based on their biological features. Assurance of confidentiality, integrity and availability of information are what information security is all about. Biometrics has come a long way to support some aspects of security such as identification, authentication and non-repudiation. These kinds of supports are crucial in systems which are reliant on individual passwords, pin identification and token based arrangements. Biometric is used to identify the veracity of an input sample when compared to a template, particularly to identify people by certain traits or characteristics[1]. Biometric authentication is fast developing field pushed by technology and threats of various kinds. In modern approach, biometric traits can be classified into two types:

- Physiological biometrics related to the shape of the body which varies from person to person. Finger prints, face recognition, hand geometry, iris recognition, ear are some of the examples under this category.
- Behavioral biometrics is related to behaviors of a person. Signature strokes, keystroke dynamics, voice are some of the examples for this class.

Quite a recent development has been to merge human perception to computer database in a brain-machine interface. This is slowly coming to be called as cognitive biometrics[1]. Biometric based authentication is becoming increasingly important particularly in computer based applications because the demand for huge sensitive data storage. Initially, biometric technologies were proposed for high-security specialist applications but are now emerging as key elements in the developing electronic commerce and online systems revolution as well as for off-line and standalone security systems. Yet another challenge is the implementation of biometric based authentication in embedded computer system applications, as the resources of such systems are becoming scare[2]. A paradigm shift is happening with the use of soft computing methodologies while inferring, matching, pattern finding, reducing the dimensionality, best feature selection, clustering and indexing of biometric data. This emerging field is aptly termed as soft-biometrics. Soft computing is oriented towards the analysis and design of intelligent systems. It is consortium of fuzzy logic, artificial neural networks and probabilistic reasoning including genetic algorithms, chaos theory and parts of machine learning and has the special attributes of approximation and dispositionality. While in hard computing, imprecision and uncertainty are undesirable

* Corresponding author:
hfl@du.se (Hasan Fleyeh)
Published online at http://journal.sapub.org/ajis

properties in soft computing, the tolerance for imprecision and uncertainty is exploited to achieve an acceptable solution at a low cost, traceability, and with a high machine intelligent quotient[3, 4].

The intent of this article is to present some vivid pictures on application of soft-computing approaches in general and to enthuse the research community to explore the realm of soft-computing as a tool for biometric applications in particular.

The presentation is organized as follows; Section 2 gives an overall view of soft computing, biometric applications of fuzzy logic is elucidated in Section 3, Section 4 showcases the applications of artificial neural networks, applications of evolutionary computing is elaborated in Section 5, Section 6 gives a presentation of applications of hybrid systems, an analysis on how soft computing techniques could be expeditiously used in biometrics is presented in Section 7 and finally we conclude this writing in Section 8.

## 2. Fuzzy Logic in Biometrics

Fuzziness refers to non statistical imprecision and vagueness in information and data. The difference between fuzzy logic and probabilistic logic consists in the fact that the fuzzy logic uses truth degrees as a mathematical model for vague facts while the probabilistic one is a mathematical model for random facts[5]. The fuzzy logic was introduced for a mathematical treatment of the vague information. The mathematical representation is based on degree of belongingness - a measure of membership in a set or to a linguistic value. A linguistic variable is a term used in natural language. The linguistic values are used for writing the rules. Researchers in this area have felt that fuzzy logic is vital to biometric authentication[6]. The simple reason attributed being that the biometric data can rarely be qualified or analyzed with hard limiters of 0 (false) or 1(true).

Biometric authentication is basically a visual activity of human experts supported by their intelligence – both of them together will ensure an excellent quality in identifying the similarity or dissimilarity among images. Further, ordinary people are not aware of the numerical reality of an image but only of certain meanings decoded according to their experience from the chromatic variation captured in the image. Therefore, for a human agent the image is not a numerical data but a set of complex knowledge about the texture of a biometric entity. Thus the inferences drawn from a pair of images by different experts vary in the degrees of precision. Probably this is the motivation for the use of fuzzy logic and for setting the goal of designing automated biometric recognition systems. In this direction, a fuzzy recognition function has been developed in an automated iris recognition application where linguistic qualifiers such as excellent approximation, very good approximation and good approximation have been graded[7, 8]. In general, the literature investigating logical aspects of image recognition or logical aspects of biometry are indeed very few. The situation when a pair of irises ambiguously belongs to both imposter and genuine fuzzy sets is investigated by Popescu-Bodorin and Balas[8].

Fuzzy logic concepts seem to be a better choice in multi-modal biometric systems (using more than one biometric feature). Multi-modal approach to biometrics will alleviate the drawbacks of each individual technique. In this context, the work of Lau et al.[9] presents a multi biometric system verification system that combines speaker verification, fingerprint verification with face identification. The authors use a fuzzy decision system in order to take into account external conditions that can affect verification performances. They show how the fusion of the three techniques reduces the error rates of 48% w.r.t speaker verification alone.

Another interesting work by De Ru and Eloff[10] is that improves security by using typing biometric to reinforce password authentication mechanism. Also this methodology employs fuzzy logic to measure the users typing biometrics. Fuzzy binary decision tree (FBDT) has been proposed by Kumar et al.[11] for the biometric based authentication system. The algorithm is used to make decision on two classes: genuine (acceptance) and imposter (reject) using matching scores computed from biometric data bases. The proposed FBDT uses fuzzy gini index and fuzzy entropy for the selection of tree nodes. In this method, the fuzzy membership functions can be automatically computed from the scores. FBDT was tested on two publicly available databases and it is reported to have fared well over its crisp counterpart.

Fuzzy logic system has been used in fingerprint identification system developed by Iancu et al.[12]. The method proposed is based on the minutiae points of the fingerprints. To reduce the search time and complexity, authors have proposed to classify the fingerprints first, and then, to identify the input fingerprints only in one subset of the data base. To choose the right subset the fingerprint is matched at a coarse level to one of the existing types. For identifying an input fingerprint, the proposed method uses a fuzzy classification of the data. Authors of this work have claimed increased efficiency of the system.

Five ways of fuzzy authentication for secure banking has been discussed by Shermila[13]. In this work, various types of authentication factors that are used in secure banking data transmissions to make more data security are discussed. The main implementation of the project is to get the fingerprint, radio frequency identification and the personal identification number (PIN) from the user for the Authentication. If the fingerprint is same but not so clear then the main server will generate the token number to the user's mobile number as one time password. This generated password would be given using key pad matrix. Server will then verify user's finger print, RFID card, PIN number and OTP via Key Pad Matrix.

## 3. Artificial Neural Networks in Biometrics

An artificial neural network is an analysis paradigm that is vaguely modeled after the massively parallel structure of the brain. It simulates a highly interconnected, parallel computational structure with many relatively simple processing elements. A well designed neural network is known for its ability to deal with noise and variable information. The four areas in biometrics where neural networks are best applicable are the classification, clustering or compression, generation of patterns and associative memory. In face recognition, it is important to select the invariant facial features especially faces with various pose and expression changes. For this novel feature extraction techniques such as entropy and mutual information have been attempted. The information so gathered has been used for classification by feed a forward neural network which has reportedly yielded better results when compared with other methods[14].

In a study that involved morphological feature extraction from hand-shape images, a pattern spectrum was used as input to recognition systems. In this study, neural networks and support vector machine (SVM) techniques were employed for identification. The verification case was analyzed through Euclidean distance classifier, obtaining the False Acceptance Rate (FAR) and False Rejection Rate (FRR) of the system for a number of *K*-fold cross validation experiments. The identification rate was found to be as high as 98.15%. The results indicated that the pattern spectrum represents a good alternative of feature extraction for biometric applications and also form pertinent input sequences for neural networks[15].

Principal Component Analysis (PCA) for ear image feature extraction and multilayer feed forward neural network has been conjointly used for classification. A framework was proposed to improve recognition accuracy of human beings. The framework combines noise filtering, PCA based feature extraction and neural network based recognition together. Furthermore the proposed framework was built on a (MFFNN). This simplicity in its architecture enables the framework to reduce the computational time. The evaluations showed that the framework achieved higher recognition accuracy with less computational time. The framework was tested on an ear image database to evaluate its reliability and recognition accuracy. The experimental results showed that the framework achieved higher stable recognition accuracy and over-performed other existing methods. The recognition accuracy stability and computation time with respect to different image sizes and factors have also been investigated[16].

Radial basis function neural network is used to perform classification task in an application related to face recognition. In this work, the curvelet transform, Linear Discriminant Analysis (LDA) were used to extract features from facial images first, and radial basis function network (RBFN) was used to classify the facial images based on features. Radial basis function network was claimed to have reduced the number of misclassification caused by nonlinearly separable classes. Around 200 images were drawn from ORL database and were tested. In this research work, RBNF was proved to be robust and has shown a recognition rate of 98.6% and acceptance ratio of 85 %[17].

An approach for accurate biometric recognition and identification of Human Iris patterns using neural network has been illustrated. For this, a template of size 10 X 480 pixels was considered. The methodology suggested has resulted in the reduction of the space requirement as well as time complexity with no loss in accuracy. Hamming distance has been used as a distance metric. Feed forward back propagation, Cascade forward back propagation, Elman forward back propagation and simple perceptron have been used. It has been established that the method suggested applying perceptron provides the best accuracy in respect of iris recognition with no additional computational complexity [18].

Attempt has been made to investigate the effects of facial artifacts on the recognition rate of Eigen face based neural networks. It has been found that Eigen faces coupled with Euclidean distance can be successfully used to recognize the human face in almost real-time, as facial artifacts can cause the features that characterize a face to be distorted. Efforts were directed to identify problematic facial artifacts that can cause false identification or no identification. The focus of this research was the investigation of common facial artifacts on the performance of recognition and the proposition of modification to existing databases to improve the positive rate of identification. A professional graphic artist was used to modify the images used in the experiments. Single and multiple Eigen face based neural network are used as classifiers[19].

In all the works cited, analytical tasks in biometrics assisted by neural networks takes its inspiration from the fact that the neural networks are universal approximators, and their ability to learn and adapt to the environment and the ability to invoke weak assumptions about the input data.

# 4. Evolutionary Algorithms in Biometrics

Evolutionary algorithms are roughly based on mechanisms of evolution such as natural selection and biological genetics. A galaxy of algorithms included under this premise are, genetic algorithms, evolutionary programming, genetic programming, evolution strategies, particle swarm optimization, artificial immune systems and the like. Evolutionary algorithms are known for their generality and robustness[3]. Varied applications of evolutionary algorithms may be found in literature. They have been applied for such problems as multiple-fault diagnosis, robot track determination, schedule optimization, conformal analysis of DNA, load distribution by electric utilities, neural network optimization, and product ingredient mix optimization. They have also been used for rule based machine learning systems and classifier systems. It is worth

mentioning that the ever going popularity of evolutionary algorithms in a variety of application domains is owing to their reputation as optimizers. Since their very inception, several researchers have attempted to use evolutionary algorithms for pattern recognition, image processing, and classification[20].

Genetic algorithm based solution was proposed for registering fingerprints in large data bases. Precisely in this work, genetic algorithms have been used to detect and adjust any rotation in the images and to further take them back to their original forms. The main objective of this research is to identify the rotation angle through genetic algorithm and to retrieve the original image knowing the coordinates of its periphery. Authors have reported that they were successful in retrieving rotation angles to an accuracy approaching 100%[21].

Genetic Algorithm (GA) has been used to face the curse of dimensionality in the event of too many biometric related features. In this context, two different GA architectures are applied to a feature selection problem in on-line signature verification. The standard GA with binary coding was first used to find a suboptimal subset of features that minimizes the verification error rate of the system. The curse of dimensionality phenomenon was investigated using a GA with integer coding. MCYT signature database comprising 330 users (16500 signatures) has been used in the study. Signatures are represented by means of a set of 100 features which can be divided into four different groups according to the signature information they contain, namely: *i*) time, *ii*) speed and acceleration, *iii*) direction, and *iv*) geometry. Authors have shown that that features from subsets *i* and *iv* are the most discriminative when dealing with random forgeries, while parameters from subsets *ii* and *iv* are the most appropriate to maximize the recognition rate with skilled forgeries[22].

Application of two evolutionary algorithms a Memetic Algorithm (MA) and GA, for feature selection for a face recognition system has been reported[23]. The algorithms were tested on two facial databases: the Cambridge ORL database and a subset of 20 subjects from the YaleB database. The Principal Component Analysis (PCA) and Linear Discriminant Analysis have been applied for feature extraction and to create the original feature templates. The Memetic and Genetic algorithms were applied in an effort to reduce the dimensionality of the feature templates as well as to increase the recognition rate. Their results showed the said algorithms outperformed the baseline methods, which used all of the extracted features, in terms of feature usage and recognition rate. Their results also showed that the Memetic algorithm outperformed the GA.

Particle Swarm Optimization (PSO) and a GA have been conjointly applied for feature selection for a facial recognition problem[24]. Images from the Cambridge ORL database were used to form a training set, which consisted of four images of each of the 40 subjects, and a test set, which consisted of six images of each of the 40 subjects. Two baseline methods, the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) methods, were then used to extract the original set of features. This research work demonstrated that the evolutionary algorithms could increase the recognition accuracy over the baseline methods while using fewer features. In addition, the PSO used fewer features than the GA.

Innovative application of two genetic evolutionary based algorithms (GEBA) for feature selection and feature weighting for facial recognition has been reported[25]. The first algorithm, referred to as Genetic & Evolutionary Feature Selection (GEFeS), evolved subsets of biometric features also in an effort to increase the recognition rate while reducing the number of features used. The second algorithm, referred to as Genetic & Evolutionary Feature Weighting (GEFeW), evolved weights for the features. These GEBAs, which were instances of a Steady-State GA and Estimation of Distribution Algorithms (EDAs), were applied to Eigen face and facial feature templates. Their results showed that GEFeS and GEFeW outperformed the baseline methods, achieving higher recognition rates while using significantly fewer features. Their results also showed that the EDA instance of GEFeW was the best performing algorithm. In addition, the LBP instances outperformed the Eigen face instances.

Alford et al.[26] in an extended work developed a hybrid GEBA for feature selection and weighting. The algorithm said to have dramatically reduced the number of features necessary for recognition, increased the recognition rate, and also evolved feature masks (FMs) that generalized well to unseen subjects. The GEBA, was applied to face-only, periocular-only, and face + periocular templates formed for subjects within the Face Recognition Grand Challenge (FRGC) database. Their results showed that the algorithm achieved higher recognition rates than the baseline methods, while using less than 50% of the extracted features. In addition, FMs evolved via the validation set performed better than those evolved via the training set.

# 5. Hybrid Methods in Biometrics

Hybrid soft computing models, which are blending of two or more soft computing, have been applied to a large number of classification, prediction, and control problems. The main intent of hybridization is to leverage the advantages of individual approaches. By combining smoothness and embedded empirical qualitative knowledge with adaptability and general learning ability, these hybrid systems improve the overall algorithm performance. These systems leverage the tolerance for imprecision, uncertainty, and incompleteness, which is intrinsic to the problems to be solved, and generate tractable, low-cost, robust solutions to such problems. The synergy derived from these hybrid systems stems from the relative ease with which we can translate problem domain knowledge into initial model structures whose parameters are further tuned by local or

global search methods. Some predominant combinations are cited in the literature are in order:

- *Fuzzy logic system tuned by neural networks*[27].
- *Fuzzy logic system tuned by evolutionary computing algorithms,* particularly to modify the membership functions[28].
- *Neural networks generated by evolutionary algorithms*[EC], specifically EC has been used to find the optimal set of weights for a given topology thus replacing back propagation, Evolve the network topology, simultaneously evolve both weights and topology, evolve the fitness function, and to select the critical input features for the neural network. An extensive review of the five application areas can be found in[29-31].
- *Evolutionary computing algorithms controlled by fuzzy logic*, specifically to translate and improve heuristic rules to manage EC parameters such as population size, selection , probabilities of crossover and mutation during their transition from exploration to exploitation[32-34]
- *Neural networks controlled by fuzzy logic*, fuzzy rule bases and fuzzy algorithms have been used to monitor the performance of NNs and modify their control parameters. For instance, FL controllers have been used to control the learning rate of neural networks to improve the crawling behavior typically exhibited by NNs as they are getting closer to the (local) minimum[35].

Application of hybrid soft computing systems in biometrics seems to be scanty. An efficient iris recognition system that employs circular Hough transform technique to localize the iris region in the eye image and cumulative sum based gray change analysis method to extract features from the normalized iris template and also fuzzy ARTMAP neural network to classify the iris codes has been proposed[36]. The results of simulations on a set of 756 eye images illustrate that an accurate and noise resistant personal identification system has been successfully designed. The proposed system achieved 0 false acceptance rate using 1800-bit binary iris codes and recognized all authorized users with 100% accuracy. In another attempt, face recognition technique using evolutionary fuzzy clustering and parallel neural networks. Evolutionary fuzzy clustering is used for optimal distribution of images into the corresponding clusters which are generated through fuzzy clustering. Parallel neural network is used for training and recognition process is done based on the outcome of the parallel neural network. For evaluation of performance of the proposed technique, AT & T bell lab face dataset has been employed[37].

# 6. The Appraisal

Needless to say that, any biometric system is characterized by copious data pertaining to features which are mired in diverse variations, measurement errors and other flaws. Therefore, such systems should be able to handle these vagaries by using tolerance mechanisms. Added to this, it should be possible to adjudge the person's/ entity's identity with a certain degree of probability or to a certain degree of truth. It is exactly here, that the soft computing techniques augur well. Soft computing techniques by their ability to consider variations and uncertainty in data are applicable for biometric systems for the following reasons.

- Biometric features sans an absolute ground truth and they will hardly reach this. Biometric features always vary.
- Derivations from the ideal biometric characteristic are difficult or even not amenable to be described analytically.
- High accuracy within the measurement may lead to inflexibility and loss of generalization ability.

Taking cue from the vast literature on applications of soft computing techniques in biometrics, it can be said that artificial neural networks seem to top the list with a larger number of applications. This is possibly due to many attractive theoretic properties of ANN. Specifically, the ability to detect non-predefined relations such as nonlinear effects and/or interactions. These theoretic advantages come at the cost of reduced interpretability of the model output. Theoretically, an ANN should have considerable advantages over other standard statistical approaches. Neural networks automatically allow arbitrary nonlinear relations between the independent and dependent variables, and all possible interactions between the dependent variables. In addition, ANNs do not require explicit distributional assumptions (such as normality, which is not seen in biometric data). These advantages have generated considerable interest in the use of neural network techniques for biometric authentication. However, there are a more number of reported researches on neural network applications in biometric classification task than any other intent.

However, ANN is not without lacunae. The primary disadvantage of an ANN is its black box quality, that is, without extra effort it is difficult if not impossible to gain insight into a problem. Researchers have alleviated this lacuna by optimizing neural network parameters such as topology, learning parameter, momentum factor with fuzzy logic and evolutionary algorithms. Invariably, such optimally evolved networks have shown very high degrees of accuracy in biometric related analytical tasks.

Fuzzy logic is widely used for human-related sciences, and successfully solves these problems. Biometrics is one of these attractive applications, which requires feature extraction and matching tasks. Especially, fuzzy logic has been successfully applied to many biometric matching systems, such as face recognition, fingerprint recognition and so on in which fuzzy logic has been shown to have achieved higher robustness, adaptively and precision. Fuzzy k-means and fuzzy vector quantization have been used for authentication schemes. Most of the applications have used type-2 fuzzy logic as it can model uncertainty and also reduce it to a minimum.

In some applications cited, fuzzy logic is used for processing of images pertaining to biometrics. One potential use has been fuzzy histogram equalization, which is

essentially gray level mapping into a fuzzy plane, using membership transformation functions. The main intent is to generate an image of higher contrast than the original image by giving a larger weight to the gray levels that are closer to the mean gray level of the image than to those that are farther from the mean.

Some researchers have used modification of membership values of to tame the vagueness in biometric image related information. After the image data are transformed from gray-level plane to the membership plane, appropriate fuzzy techniques are used to modify the membership values. It could be fuzzy clustering, a fuzzy rule-based approach, and a fuzzy integration approach. In some cases, fuzzy filters have provided promising result in image-processing tasks that cope with some drawbacks of classical filters. Fuzzy logic has also been augmented to recover a heavily noise corrupted image. Each pixel in the image is represented by a membership function and different types of fuzzy rules that considers the neighborhood information or other information to eliminate corrupted pixels. Fuzzy filters have also been found to perform both the edge preservation and smoothening.

**Table 1.** A summary of Case Studies

| Nature of Biometric Work and soft computing method adopted | Findings | Reference |
|---|---|---|
| 1. Novell models for all steps of a face recognition system. In the step of face detection, hybrid model combining AdaBoost and Artificial Neural Network to solve the process efficiently. In the next step, labeled faces detected by ABANN were aligned by Active Shape Model and Multi Layer perceptron. In this alignment step, a new 2D local texture model based on Multi Layer Perceptron has been. Further in feature extraction step, a methodology for improving the efficiency by the association of two methods: geometric feature based method and Independent Component Analysis method have been described. In the face matching step, a model combining many Neural Networks for matching geometric features of human face has been proposed. The model links many Neural Networks together, and it is ascribed as Multi Artificial Neural Network. MIT + CMU database is used for evaluating the proposed methods for face detection and alignment | The classifier of the model significantly improved the accuracy and the robustness of local searching on faces with expression variation and ambiguous contours.<br>No of faces recognized : 466<br>ANN Structure: Based on Rowley's model.<br>Detection Rate : 92%<br>Average time to process an image: 0.174 seconds. | Le[38] |
| 2. Hand-shape biometric system using neural networks and support vector machines, and a novel feature extraction based on the morphological pattern spectrum has been reported. Authors have done an extensive comparison with results obtained from different feature extraction methods reported in the literature and have showed a very competitive performance by the method suggested by them. The properties of invariance to rotation and position of the pattern spectrum has also been considered. This will allow the user to pose naturally the hand without additional constraints. | The network architecture used in this work composed 25 input nodes, a hidden layer of 25 nodes, and 20 output nodes. All neurons used a sigmoid as an activation function. Single-layer perceptron trained with the Levenberg–Marquardt back propagation algorithm. A two fold cross validation scheme was used. The training algorithm showed fast convergence | Cortes et al.[16]. |
| 3. An optimized method to reduce the number of points to be used in order to identify a person using fuzzy fingerprints. Two fingerprints are similar if n out of N points from the skin are identical. Method based on fuzzy logic is used and compared with the classical methods applied on fingerprints. The method compares two matching sets and selects the optimal set from these, using a fuzzy reasoning system. | The advantage of the method with respect to the classical existing methods is smaller number of calculations. | Inchu et al.[12] |
| 4. Two different Genetic Algorithm (GA) architectures are applied to a feature selection problem in on-line signature verification. The standard GA with binary coding is first used to find a suboptimal subset of features that minimizes the verification error rate of the system. The curse of dimensionality phenomenon is further investigated using a GA with integer coding. Results are given on the MCYT signature database comprising 330 users (16500 signatures). Signatures are represented by means of a set of 100 features which are divided into four different groups according to the signature information they contain, namely: *i*) time, *ii*) speed and acceleration, *iii*) direction, and *iv*) geometry. | The research indicated that features from subsets *time* and *geometry* are most discriminative when dealing with random forgeries, while parameters from subsets speed and *acceleration* and *geometry* are the most appropriate to maximize the recognition rate with skilled forgeries. | Galbally et al.[22] |

Evolutionary Biometrics is an emerging sub-area that is devoted to the design, development, and application of Darwinian-style methods (those based on natural selection) for solving problems within the area of biometrics. Evolutionary algorithm assisted biometrics is deemed to discover optimal or near optimal solutions to problems. Evolutionary algorithms find befitting application because biometric feature extraction is essentially a kind of optimization problem. Literature survey revealed the wide application of genetic algorithms. Researchers have found the advantage of potential parallelizability with these algorithms and thus their applicability on large-scale and high-dimensional data. Face recognition, finger print recognition and Iris recognition have found to be the major applications of evolutionary feature extraction. Evolutionary pursuit is successfully applied to face recognition and achieved a better performance than the popular Eigen face related methods. In our view, evolutionary methods are more apt owing to the following reasons:

- They work with a coded parameter sets and not with the parameters themselves.
- Searching is over a population of candidate solutions, not a single point.
- Algorithm uses objective function information, not derivative or other auxiliary information.
- Algorithms use probabilistic transition rules, not deterministic rules.
- The result is a population of solutions instead of an individual solution.

However, wide spread utility of other paradigms of evolutionary techniques such as Particle swarm , Honey bee colony, Ant colony, Termite colony, Bacterial foraging algorithms are the open areas still to be explored by prospective researchers in this field.

Literature survey also revealed a scanty application of hybrid systems involving more than one of the soft computing components. Most of the reported works relate to blending of ANN with other component(s). Genetic algorithms are used either to train networks or for simultaneous evolution of the network's weights and topology. Fuzzy logic has been used to control the learning rate of neural networks to improve the crawling behavior typically exhibited by NNs as they are getting closer to the (local) minimum. Thus improvement of efficacy of biometric systems through hybrid algorithms is still an open area for researchers to explore. A few typical case studies are presented in Table 1.

## 7. Conclusions

In this article we have underlined the importance and significance of soft computing paradigms in biometric schemes. This article is also driven by the renewed demands from biometric systems such as robustness, higher recognition rates, and tolerance for imprecision, uncertainty and flexibility which calls for new computing techniques. Soft computing assisted biometrics has been successful in data representation, dimensionality reduction, feature selection, mapping and other kind of analytics. It is felt that the prospective researchers in the area of biometrics are encouraged by this article and further explore soft computing based algorithms in the future development of biometric technologies.

## REFERENCES


[1] D. Bhattacharyya, R. Ranjan, F. Alisherov, M. Choi, Biometric authentication: A Review, International Journal of u-and e-Service, Science and Technology, 2(3), pp 13-28. , 2009

[2] M. Malcangi, Soft computing methods for robust authentication using soft-biometric data, Neural Computation & Application, Springer, 2011.

[3] J. Rudas, J. Fodor, Intelligent Systems, Int. Journal of Computers, Communications & Control, 3(1), pp 132-138, 2008.

[4] C. Altrock, Fuzzy logic and Neuro fuzzy applications explained, Upper Saddle River, NJ, Prentice Hall, 1995.

[5] N. Constantinescu, I. Iancu, Fuzzy Identity Authentication, Latest Trends on Computers, 1(1), pp 168-173, 2008.

[6] N. Bodorin, V. Balas, 8-Valent Fuzzy Logic for Iris Recognition and Biometry, Proc.5th IEEE Int. Symp. On Computational Intelligence and Intelligent Informatics, Floriana, Malta, 2011.

[7] N. Bodorin, V. Balas, Learning Iris Digital Biometric Identities for Secure Authentication, Recent advances in Intelligent Engineering Systems, Springer Verlag, 2011.

[8] N. Bodorin, V. Balas, Exploratory Simulation of an Intelligent Iris Verifier Distributed System, Proc. 6th IEEE International Symposium on Applied Computational Intelligence and Informatics, IEEE press, pp.259-262, 2011.

[9] C. Lau, B. Ma, H. Meng, Y. Moon and Y. Yam, Fuzzy Logic decision Fusion in a Multimodal Biometric System, Proc. 8th International Conference on Spoken Languages Processing, Korea, 2004.

[10] W. De Ru , J. Eloff, Enhanced Password Authentication Through Fuzzy Logic, IEEE Expert, 12(6), pp 38-45, 1997.

[11] A. Kumar, M. Hanmandlu, Das. A, H. Gupta, Biometric Based Personal Authentication using Fuzzy Binary Decision Tree, Proc. 5th IAPR Int. Conf. on Biometrics, Delhi, India, pp 396-401, 2012

[12] I. Iancu, N. Constantinescu, M. Colhon, Finger Prints Identification using a Fuzzy Logic System, Int. J. of Computers, Communications & Control, 5(4), pp 525-553, 2010.

[13] S. Jennifer, R. Shermila, A five-ways fuzzy authentication for secured banking, International Journal of Engineering Research and Application, 2(4), pp 375-379, 2012.

[14] S. Kakarwal, R. Deshmukh, Information theory and Neural

Network based approach for face recognition: A review, Int.Journal of Recent Trends in Engineering, 2(4), pp 176-178. 2009

[15] J. Cortes, P. Gil, V. Aquino, D Lopez, R. Galdera, A Biometric System Based on Neural Networks and SVM Using Morphological Feature Extraction from Hand-Shape Images, Informatica, 22(2), pp 225-240. 2011

[16] M. Alaraj, J. Hoe, T. Fukami, A Neural Network based Human Identification Framework Using Ear Images, IEEE-TENCON, pp 1595-1600, 2010.

[17] V. Radha, N. Nallammal, Neural Network Based Face Recognition Using RBNF Classifier, Proc. World Congress on Engineering and Computer Science, Vol. I, San Francisco, USA. 2011

[18] M. Gopalakrishnan, T. Sanathanam, Improved Biometric Recognition and Identification of Human Iris Patterns using Neural Networks, Journal of Theoretical and Applied Information Technology, 31(2), pp134-139, 2011.

[19] K. Sundaraj, Investigation of Facial Artifacts on Face Biometrics using Eigenface based Single and Multiple Neural Networks, WSEAS Transactions on Systems, 8(1), pp 127-136, 2009.

[20] C. Coello, Evolutionary Algorithms: Basic Concepts and Applications in Biometrics, Synthesis and Analysis in Biometrics, World Scientific Publishing, pp 1-34, 2006,

[21] Ibrahiem, E. Emery, M El-Kareem, On the application of Genetic Algorithm in Finger Print Recognition, World Applied Sciences Journal, 5(3),pp 276-281, 2008.

[22] J. Galbally, J. Fierrez, M. Freire, J. Garcia, Feature Selection based on genetic Algorithms for on-line signature verification, Lecture Notes in Computer Science, Vol 5845, pp 246-257, 2009.

[23] D. Kumar, S. Kumar, S. Rai, Feature Selection for face recognition: A Memetic algorithm approach, Journal of Zhejanga University Science, 10(8), pp 1140-1152, 2009.

[24] R. Ramadan, F. Abdel-Kader, Face Recognition Using Particle Swarm Optimization-Based Selected Features, Int. Journal of Signal Processing, Image Processing and Pattern recognition, 2(2), pp 51-66, 2009.

[25] T. Abegaz, , G. Dozier, K. Bryant, J. Adams, V. Mclean, J. Shelton, A. Alford, K. Ricanek, D. Woodard, Applying GECs for Feature Selection and Weighting using X-Tools, Proc. of 8th Annual International Conference on Genetic and Evolutionary Methods, pp 1-6, 2011.

[26] A. Alford, C. Steed, M. Jeffrey, D. Weet, J. Shelton, L. Small, D. Leflore, Dozier, G. Bryant , T. Abegaz, J. Kelly, K. Ricanek, Biometrics: Hybrid Feature Selection and Weighting for a Multi-Modal Biometric System, Proc. of IEEE Southeast Con, pp 1-8,2012.

[27] J. Jang, ANFIS: Adaptive-network-based-fuzzy inference system, IEEE Trans. On Systems, Man, and Cybernetics, 23(3), 1993, pp 665-685.

[28] O. Cordon, H. Herrera, and M. Lozano, A Classified review on the combination fuzzy logic- genetic algorithms bibliography, Tech. Report 95129, Department of Computer Science and AI, Universidad de Granada, Granada, Spain, 1995, Available at : http://decsai.ugr.s/~herrera/flga.html.

[29] V. W. Port, Overview of Evolutionary Computation as a Mechanism for Solving Neural System Design Problems, Hand Book of Neural computation, Oxford University Press, 1997.

[30] E. Vonk, L. Jain, and R. Johnson, Automatic Generation Neural Network Architecture Using Evolutionary Computation, World Scientific Publication, 1997.

[31] X. Yao, Evolving Artificial Neural Networks, IEEE Trans. On Neural Networks, 87(9), 1999, pp 1423-1447.

[32] C. Karr, Design of an adaptive fuzzy logic controller using genetic algorithms, Proc. Int. Conf. on Genetic Algorithms, San Diego, 1991, pp 450-456.

[33] M. Lee , H. Tagaki, Dynamic control of genetic algorithm using fuzzy logic techniques, Proc. Fifth Int. Conf. on Genetic Algorithms, Morgan Kaufmann, CA, 1993, pp 76-83.

[34] H. Surmann, Kanstein, K. Goser, Self-organizing and genetic algorithms for an automatic design of fuzzy control and Decision Systems, Proc. EUFIT, Germany, 1993, pp 1097-1104.

[35] P. Arabshahi, J. Choi, R. Marks, and T. Caudell, Fuzzy control of Back Propagation, Proc. IEEE Int.Conf on Fuzzy Systems, San Diego, 1992, pp 967-972.

[36] A. Taherian, M. Aliyarish, Noise Resistant Identification of Human Iris Patterns Using Fuzzy ARTMAP Neural Network, Int. Journal of Security and Its Applications, 7(1), pp 105-118, 2013.

[37] V. Srivastava, B. Tripathi, V. Pathak, Evolutionary Fuzzy Clustering and Parallel Neural Networks based Human Identification using Face Biometrics, Int. Journal of Computer Applications, 31(7), pp 1-6,2011.

[38] T. Le, Applying Artificial Neural Networks for Face recognition, Advances in Artificial Neural Networks, Vol. 2011, 2011,pp 1-16