Enhancing The Performance Of Neural Network Classifiers Using Selected Biometric Features

Heman Mohabeer, K.M. Sunjiv Soyjaudah and Narainsamy Pavaday
Faculty of Engineering
University of Mauritius
Reduit, Mauritius
heman.mohabeer@gmail.com, ssoyjaudah@uom.ac.mu, n.pavaday@uom.ac.mu

***Abstract*— This paper describes an application which increases the overall efficiency of a neural network classifier intended for authentication whilst using fewer biometric features. Normalization of the biometric data is generally performed to remove unwanted impurities. However, in this case, when performing normalization, the statistical property for each set of data has also been taken into consideration prior to the classification process. Combination of the normalized biometric features has been performed while comparing their standard deviation. The resulting fused data has correlation value as low as possible. This gives rise to a higher probability of uniquely identifying a person in feature space. The proposed system is intended to make authentication faster by reducing the number of biometric features without degrading the overall performance of the classifier. The performance of the classifier was computed using the mean square error (MSE). The results show that redundant biometric data can indeed be excluded without degrading the performance of the classifier.**

Keywords-mean square error; normalization; biometric sample; keystroke dynamics.

I. INTRODUCTION

Biometric systems have been successfully applied as a method of authentication to replace conventional access controls [1][2]. Biometrics is the automated method of recognizing a person based on physiological or behavioral characteristics. Biometric data are highly unique to each individual, easily obtainable non-interferingly, time invariant (no significant change over a period of time) and distinguishable by human without much special training [3]. Enrollment and authentication are the two primary processes involved in a biometric security system. Enrollment consists of biometric measurements being captured from a subject. The related information from the raw data obtained from the subject is gleaned by the feature extractor, and this information is stored on the database. During authentication, biometric information is detected and compared with the database through pattern recognition techniques [4][5][6] that involve a feature extractor and a biometric matcher working in cascade.

Biometric technologies were first proposed for high security applications [6][7], but are now emerging as key elements in the development of user authentication. These technologies are expected to provide important components in regulating and monitoring access [7]. Momentous application areas include security, monitoring, database access, border control and immigration. Until now, biometric systems have been relatively expensive. In addition, they have lacked the required speed and accuracy. A family of techniques has emerged, where quality measures were used to weigh the contribution of different biometric modalities in multi-modal fusion [8]. Quality measures have also been heuristically included as meta-parameters in biometric matchers. More recently, quality measures have been interpreted as conditionally-relevant classification features and used jointly with other features to train statistical models for uni-modal and multi-modal biometric classification [9][10][11].

In this paper, we propose a novel technique for selecting biometric features for authentication purposes. The statistical property of each feature has been taken into account. The aim has been to unambiguously identifying each individual enrolled in the system while decreasing the number of features used for authentication purposes. This obviously leads to faster authentication and also an improvement in performance. Data mining technique have been used to remove unwanted impurities (noise, etc.) from the data. The variance and standard deviation of the refined data have been computed. The result shows that the statistical properties of biometric data can play an integral role in the accuracy and performance of classification. Section two provides a literature of the concept of data mining technologies and the z-score normalization technique. Section three provides the methodology of the approach used in the design of the system. Section four shows the results of the simulation and Section five provides ground for discussion and future work while section six gives an insight of the impact this research.

II. DATA MINING TECHNOLOGIES

Generally, data mining means the extraction of hidden predictive information from large databases. This is a powerful new technology with great potential to help companies focus on the most important information in their data warehouses [12]. Data mining tools predict future trends and behaviors, allowing businesses [13] to make proactive knowledge-driven decisions. They scour databases for hidden patterns, finding predictive information that experts may miss because these information lies outside their expectations. Data transformation such as normalization may improve the accuracy and efficiency of mining algorithms involving neural networks, nearest neighbor and clustering classifiers [14]. Score normalization

 ISBN: 978-1-61208-144-1

refers to changing the location and scale parameters of the matching score distributions at the outputs of the individual matchers [15]. The resulting output is used to perform classification, so that the matching scores of different matchers are transformed into a common domain. The most commonly used score normalization technique is the *z-score* [17]. This calculated using the arithmetic mean and standard deviation of the given data. This scheme can be expected to perform well if prior knowledge about the average score and the score variations of the matcher is available [16]. If we do not have any prior knowledge about the nature of the matching algorithm, then we need to estimate the mean and standard deviation of the scores from a given set of matching scores. The normalized scores (S_k') are given by [17]

$$S_k' = (S_k - \mu)/\sigma$$

where S_k is the raw data, μ is the arithmetic mean and σ is the standard deviation of the given data. If the input scores are not Gaussian distributed, *z*-score normalization does not retain the input distribution at the output. This is due to the fact that mean and standard deviation are the optimal location and scale parameters only for a Gaussian distribution [18].

III. METHODOLOGY

The flowchart shown in Fig.1 provides an insight of the design of the application. A hold is a distinct biometric feature from a biometric sample. The biometric data labeled 1, 2 and three consisted of different features or hold. Fig. 2 shows the histogram of the distribution of hold one which indeed follows a Gaussian distribution hence z-transform is a possible standardization for the data. It is a set of input which is similar for different individual.

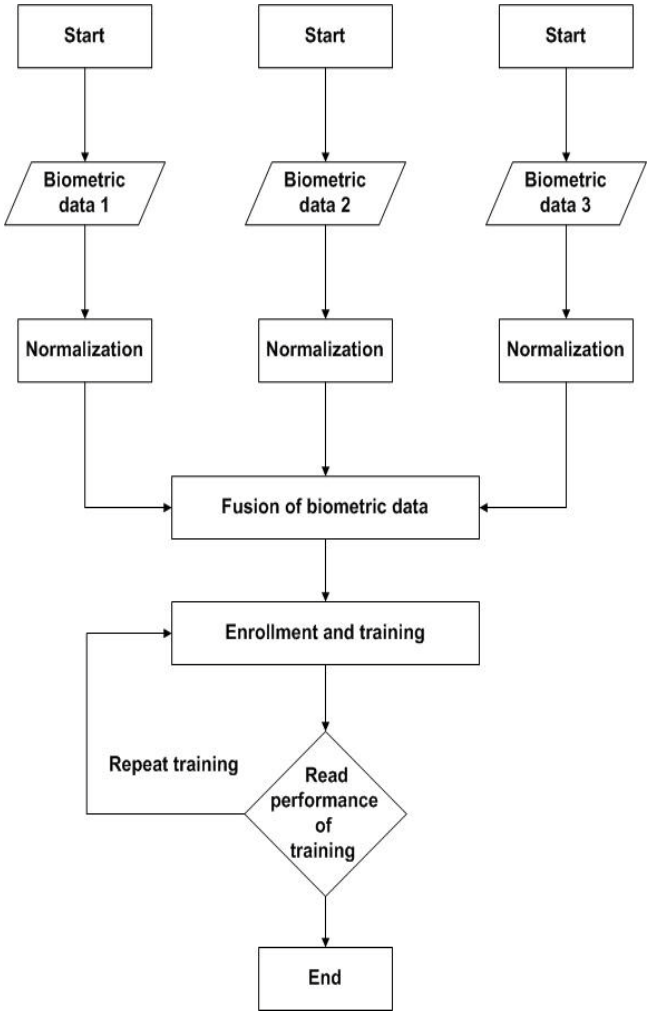

Figure 1. Flowchart showing the design of the system

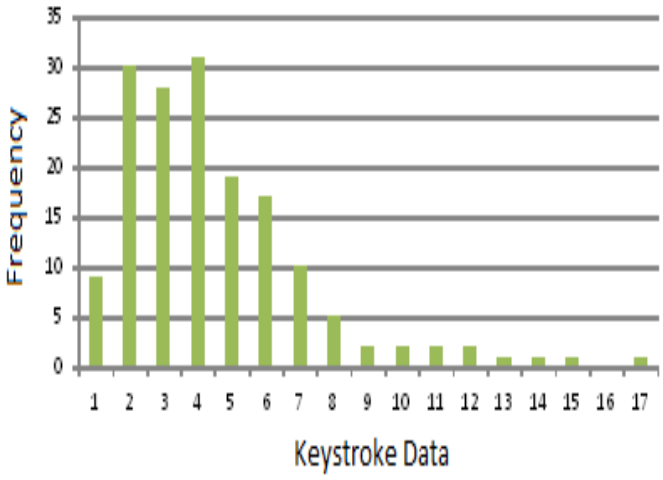

Figure 2. Plot of frequency distribution against data for Hold 1

 ISBN: 978-1-61208-144-1

Table 1 shows the mean and the standard deviation for each feature, in this case defined as holds. The dataset consist of nine features (hold) out of which 511 combination can be made. A subset of this amount, that is, those with greater difference in standard deviation and mean were combined for simulation purposes. This enabled a greater variance among data which decreased the correlation and thus increased the divergence from similarity for each user. This allows authentication with smaller False Acceptance rate (FAR) since there are considerable gaps between the users dataset in terms of standard deviation. It is also noticed that some features can be eliminated since they have close correlation with others and do not have a considerable impact in authentication. By eliminating these features the authentication is expected to be much faster as it makes use of fewer biometric features with more valuable information. Combining the feature vector from each biometric creates a vector that has a higher dimensionality and higher probability of uniquely identifying a person in feature space

TABLE I. MEAN AND STANDARD DEVIATION FOR EACH HOLD

Features	Average (μ)	Standard Deviation (σ)
Hold 1	9.54	2.82
Hold 2	8.34	1.83
Hold 3	8.16	1.83
Hold 4	9.07	2.82
Hold 5	10.85	4.09
Hold 6	10.04	3.01
Hold 7	9.48	3.23
Hold 8	10.43	3.36
Hold 9	8.21	1.76

IV. SIMULATIONS AND RESULTS

Simulations of the combined features were performed using neural network toolbox in MATLAB. The number of neurons, training set, and testing sets were initially chosen at random until a good and consistent result was obtained. The aforesaid parameters were eventually set to be fixed. The training algorithm used was the Levenberg Marquart algorithm and the results were computed in terms of mean square error (MSE).

Fig. 3 shows the results after the combination of two sets of data. The continuous curve is the combination with the greatest difference in standard deviation and mean while the broken curve is the combination with the smallest difference in mean and no difference in standard deviation. A horizontal line is drawn at MSE equals 0.04 to help in noting the difference between the two curves since they are closely overlapped to each other. This makes differentiation between them much easier than by mere observation of the graphs. The horizontal line is drawn as a reference to enable computation of the distinction of the two curves in a more simplified manner. The number of MSE for the red curve below the horizontal line is 50, which are about 72% of the results after simulations while the blue curve contains only 35 MSE below four representing 50% of the results both obtained upon seventy trainings

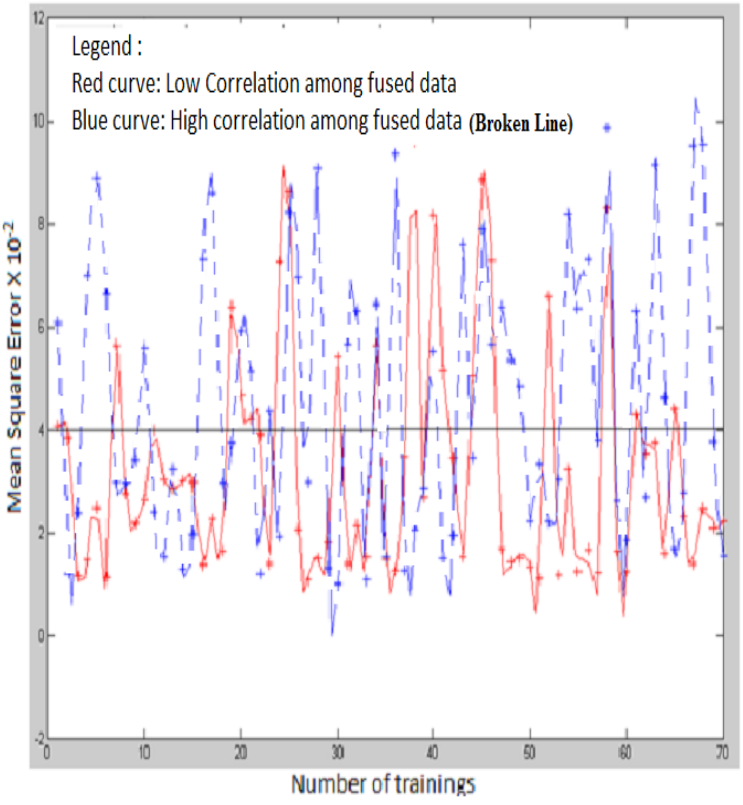

Figure 3. Performance of two sets of data combinations

Fig. 4 displays the mean square error of normalized data versus number of training for the best and worst training performances. The blue dots represents the results of the best combination whereby having greater statistical among the features. The best performance is obtained upon combining Hold 1, Hold 3 and Hold 5. This was obtained upon simulation of the combined holds. It should be noted that the correlation among these three set of data is indeed smaller compared to other combination of data. Two lines have been drawn joining the MSE for the first training and the last training. The sole purpose of the line is to show that even though the performance is continually being improved after each training, yet the combination with the lowest correlation always remained the best in terms of MSE.

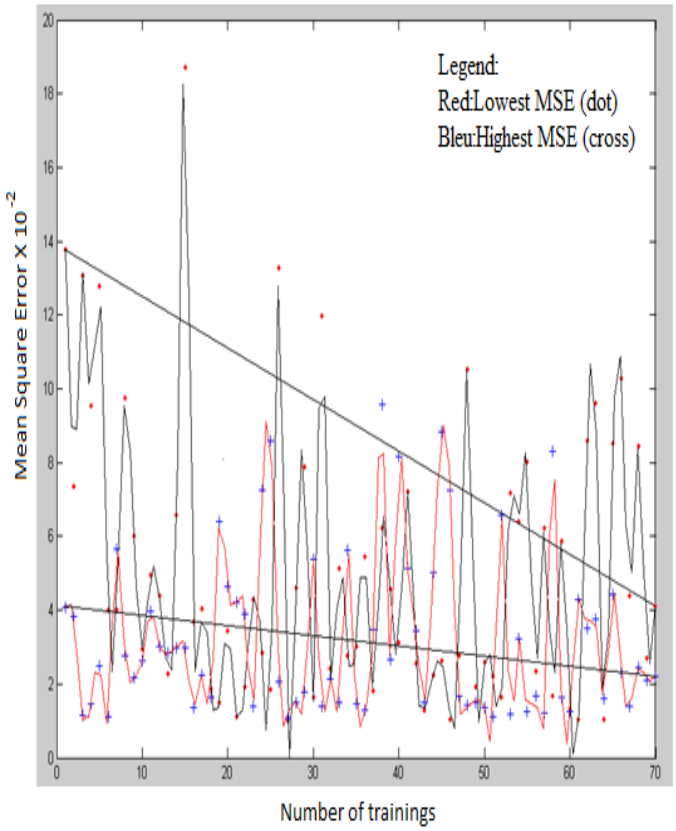

Figure 4. Mean square error of normalized data versus number of training for the best and worst training performances.

V. Discussion and Future work

Fusion of a minimal number of biometric features in order to give better performance can be made upon a good statistical analysis of the biometric data. However, too few fused features also result in poor performance. This is because of the limitation of the variation among users thus classification becomes more error prone. For this reason there must be a balance between the statistical property and the amount of features used. The search space for the individual when performing authentication should be coherent with the number of features used as this helps distinction among individuality. While reduction of the search space remains a big challenge in biometric databases, it should not be compromised with the efficiency of the system. Minimizing the number of biometric can be regarded as a good tradeoff while keeping the search space constant. In the case of keystroke dynamics, the combination of the holds resulting in their better performance could pave way for faster authentication. It would be interesting to see the behavior of the classification process in neuroevolution of augmented topologies (NEAT). NEAT also eliminates the randomness involved in selecting the topology and weight since it enables automating the process of topology and weight optimization which is expected to give an even enhanced performance. The process of complexification from a simple topology, ensure that the final architecture is rightly suited for optimal classification process. This also results in a network that is neither too big which gives rise to over fitting nor too small, resulting in under fitting. Furthermore, selections of features were made from a single type of biometric, i.e., keystroke dynamics. It opens door for fusion of different biometrics as this will obviously result in an even more enhanced performance. The reason is due to the fact that it will create even higher divergence among the data used thus creating more uniqueness among individuals. Thus, fusion of biometrics such as iris scan and fingerprint using their statistical values can be made while keeping the number of fused features low.

VI. Conclusion

In this era, security has become a key element which is kept in mind when designing and developing new technologies. Biometrics has become an emergent aspect of security hereby responding to the growing need for authentication and distinction among individualities. They are gradually taking the place of traditional authentication method. Biometric authentication has become an integral part of everyday life and the trend toward a more efficient and less time consuming device is an engineer's objective. The methodology used in this paper could inspire to build biometric systems that uses captured biometric sample and uses their statistical property to combine or remove any redundant data

Acknowledgment

The financial contribution of the Tertiary Education Commission is gratefully acknowledged.

REFERENCES

[1] Fernando L. Podiol and Jeffrey S. Dunn, Biometric Authentication Technology: From the Movies to Your Desktop, 2002

[2] Robby Fussell, Authentication: The Development of Biometric Access Control, The ISSA journal, July 2005.

[3] Jain LC, Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999.

[4] Andrijchuk, V.A. Kuritnyk, I.P Kasyanchuk, M.M Karpinski, and M.P Kasyanchuk, "Modern Algorithms and Methods of the Person Biometric Identification," Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 05), Sept. 2005, pp. 403 – 406.

[5] Jain A.K, "Biometrics: Proving Ground for Image and Pattern Recognition," Image and Graphics Fourth International Conf. (IGIG07), Aug. 2007, pp. 3-3, DIO: 10.1109/ICIG.2007.195.

[6] W. Shen and T. Tan, "Automated Biometrics based person identification," Proc. Natl. Acad. Sci. (PNAS99) , Vol. 96, pp. 11065-11066, September 1999.

[7] Simon Liu and Mark Silverman, "A Practical Guide to Biometric Security Technology," www.lfca.net, April 2001, accessed on 20/04/2011.

[8] L. Hong, A. Jain, and S. Pankanti, "Can multibiometrics improve performance?," Proc. of AutoID, 1999, pp. 59-64.

[9] J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia, and A. K. Jain, "Incorporating image quality in multi-algorithm fingerprint verification," Proc. of the ICB, Jan. 2006, pp. 213-220.

[10] J. P. Baker and D. E. Maurer, "Fusion of biometric data with quality estimates via a Bayesian belief network," Biometric Consortium Conf. Arlington, 2005, pp. 21-22 .

[11] K. Nandakumar, Y. Chen, S. C. Dass, and A. K. Jain, "Quality-based score level fusion in multibiometric systems," Proc. of ICPR, vol. 4, Aug. 2006, pp. 473–476.

[12] Berry M.J.A and Linoff, Data Mining Techniques: For Marketing, Sales, and Customer Support, John Wiley & Sons, 1997.

[13] http://www.thearling.com/text/dmwhite/dmwhite.htm, accessed on 20/04/2011.

[14] Han J. and M. Kamber, Data Mining: Concepts and Techniques, Morgan Kaufmann, 2001.

[15] Luai Al Shalabi, Zyad Shaaban, and Basel Kasasbeh, "Data Mining: A Preprocessing Engine," Journal of Computer Science 2 (9), 2006, pp. 735-739.

[16] A.K. Jain, K. Nandakumar, and A. Ross, "Score Normalization in Multimodal Biometric Systems," Pattern Recognition, Vol. 38, No. 12, December 2005, pp. 2270-2285.

[17] F. Alsade,N.zaman,M. Z. Dawood, and S. H. A. Musavi, "Effectiveness of score normalisation in multimodal biometric fusion," Journal of ICT,Vol 3,No 1, 2009, pp. 29-35.

 ISBN: 978-1-61208-144-1