International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:1, No:5, 2007

Using Data Fusion for Biometric Verification

Richard A. Wasniowski

***Abstract*—** A wide spectrum of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual person. This paper considers multimodal biometric system and their applicability to access control, authentication and security applications. Strategies for feature extraction and sensor fusion are considered and contrasted. Issues related to performance assessment, deployment and standardization are discussed. Finally future directions of biometric systems development are discussed.

***Keywords*—** Multimodal, biometric, recognition, fusion.

I. Introduction

BIOMETRIC recognition refers to the automatic recognition of individuals based on their physiological and behavioral characteristics. Current biometric systems make use of identifiers such as fingerprints, hand geometry, iris, face and voice to establish an identity. A biometric system that uses a single biometric trait for recognition has to contend with problems related to non-universality of the trait, attacks, large intra-class variability, and noisy data [10, 11, 12, 14]. Some of these problems can be addressed by integrating the evidence presented by multiple biometric traits of a user for example face and iris. Such systems, known as multimodal biometric systems, demonstrate improvement in recognition performance. Biometrics can also be defined as measurable characteristics of the individual based on their physiological features or behavioral patterns that can be used to recognize or verify their identity. Biometric technologies were first proposed for high security applications but are now emerging as key elements in the developing of user authentication. These technologies will provide important components in regulating and monitoring access. Significant application areas include security monitoring, database access, border control and immigration, forensic investigations and telemedicine. Until recently biometric machines have been relatively expensive. In addition they have lacked the required speed and accuracy except in special circumstances or with extensive user training. More recently the situation has improved with the introduction of machines that are less expensive and are improved in performance.

Manuscript received March 31, 2005. R. A. Wasniowski is with the Computer Science Department, California State University, Carson, CA 90747.

While some commercial biometric products have become available, most of these technologies are still in a research and in the experimental stage. More research and development work is required to improve their robustness and increase their performance for specific applications. This paper presents research on fusion for person identification.

II. Biometric Systems

Several different biometric modalities have emerged in recent years. Typical biometric identification and recognition systems (see Fig. 1) may have the following components: a) A sub-system for capturing samples of the biometric(s) to be used. This could be voice recordings or facial images. Specific features are extracted from the biometric samples to form templates for future comparisons. b) The templates thus obtained are stored for future comparison. This may be done at the biometric capture device or remotely in a server accessible via a network. c) The captured live biometric from the user is compared with the claimed identity which may be provided by entering stored identity information. d) There is the need for interconnections between the capture device and the verification and storage components of the system. Often there are existing access controls and information systems into which the biometric system may have to be integrated. It is important to note that some techniques, such as retinal scanning or finger print recognition, may offer high accuracy but may not be appropriate for some applications. This is due to the high level of cooperation required by the user, or the social or psychological factors that may prove unacceptable to potential users. Both voice and face recognition are considered to be easy to use and normally acceptable by potential users. However, their accuracy is currently less efficient than some other biometric technologies, especially in unconstrained environments. There are two distinct phases of operation for biometric systems: enrolment and verification identification. In the first phase identity information from the users is added to the system. In the second phase live biometric information from the users is compared with the stored records. The following are some of the key issues that need to be considered in designing and applying biometric systems. Robustness: It is important to consider how robust the system is to fraud and impersonation. Acceptability: The technology must be easy to use during both the enrolment and comparison phases. Legal issues may also have to be considered in relation to biometric systems. There may be concerns over potential intrusions into private lives by using biometric systems. Speed and Storage Requirements: The time required to enroll, verify or identify a person is of critical importance to the acceptance and applicability of the system. Integration: The hardware platform on which the system is to be implemented is a key concern.

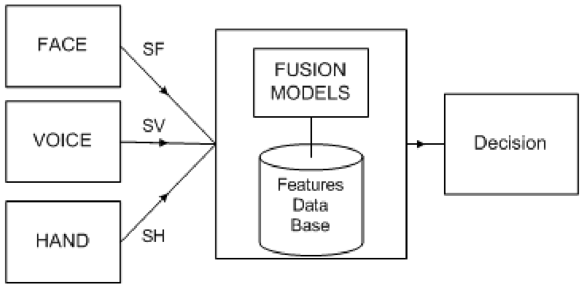

Fig. 1 Biometric recognition system

An important issue for the adoption of biometric technologies is to establish the performance of individual biometric modalities and overall systems in a credible and objective way. False Acceptance Rate - FAR is defined as the ratio of impostors that were falsely accepted over the total number of impostors tested described as a percentage. This indicates the likelihood that an impostor may be falsely accepted and must be minimized in high-security applications. False Reject Rate- FRR is defined as the ratio of clients that are falsely rejected to the total number of clients tested described as a percentage. This indicates the probability that a valid user may be rejected by the system. Ideally this should also be minimized especially when the user community may be put-off from using the system if they are wrongly denied access. A number of databases have been developed for the evaluation of biometric systems. The XM2VTS database is an example of the European solution in the domain. Developing new assessment strategies that allow meaningful comparisons between systems and solutions is an essential activity. This involves creating databases and putting together test procedures and systems for the online assessment of biometric technologies. One problem with using face or voice recognition is the robustness of these techniques to variable environmental conditions and to impersonation. It is possible to reduce the effect of these factors considerably by employing face and voice recognition concurrently and co-operatively. Such multimodal systems can be shown to be less sensitive to variations in speech patterns of a particular individual, to background noise, poor transmission conditions in remote applications and to determined attacks by impostors. In voice recognition the audio signal is sampled and quantized before feature extraction. A telephone quality system may be adequate for recognition purposes. Facial recognition has attracted a great deal of attention from researchers and continues to be an active research area. There are a number of problems associated with facial recognition. First the presence of a face or faces in a scene must be detected. Once the face has been detected it must be localized, and a normalization process may be required to bring the dimensions of the live facial sample and the one on which the template is based into alignment. Various architectures have been used for performing such classifications. There is usually a training phase where the classifier is given valid feature vectors and their associated identity tokens. Normally, the success of the operational phase depends on the quality of this training phase.

III. Fusion Systems

Recognition verification based on any one of modalities alone may not be very robust whilst combining information from a number of different biometric modalities may well provide higher and more consistent performance levels. In addition to this, any one modality may not be acceptable by a particular user, group or in a particular situation or instance. By combining modalities, greater robustness can be obtained while providing a measure of adaptability to given circumstances. Several approaches can be adopted for combining the different modalities [8, 21, 23]. The two main approaches are called feature fusion and decision fusion; also called early and late fusion. A simple approach to decision fusion will be to treat the two modalities independently. For example, in an access control application, voice verification can be performed and if successful face verification can follow. If the latter is also successful then access can be granted. In such a sequential arrangement, the latter will only be applied if the earlier verification is successful. Alternatively, both biometric technologies can be invoked, possibly concurrently in a parallel system. The system can be arranged in such a way that if any of the modalities produce an acceptance, then the user is accepted and the other layers need not be invoked. It is also possible to have a logical operation performed at the final stage to combine the decisions. A more sophisticated version of decision fusion will hold information about the performance of individual classifiers, their strengths and weaknesses in identifying/verifying particular individuals, or just under special circumstances. When it comes to combining the decisions from the different classifiers, these additional sets of performance information are combined in an optimal way to give appropriate weighting to the different biometric modalities. Alternatively in feature fusion, the feature vectors obtained from samples are used together to train a combined classifier. The advantage of this is that all the feature information is present at the classification stage. The issue of efficient and effective combination of biometric modalities is still outstanding and attracts research attention. We are applying the support vector machine approach for efficient combination of modalities. The support vector method was developed to construct separating hyper planes for pattern recognition problems. The main idea of the SVM approach is to map the training data into a high dimensional feature space in which a decision boundary is determined by constructing the optimal separating hyper plane. Computations in the feature space are avoided by using a kernel function. The formal goal is to estimate the function f: R-> {+1,-1} using input/output training data such that f will correctly classify examples. Support Vector classifiers are based on the class of hyper planes and corresponding to the decision function. The unique hyper plane with maximal margin of separation between the two classes is called the optimal hyper plane. The optimization problem thus is to find the optimal hyper plane. If function f is a nonlinear function, one possible approach is to use a neural network, which consists of a network of simple linear classifiers. Problems with this approach include many parameters and the existence of local minima. A detailed description of the version of algorithm and experiments can be located in [21]. The SVM approach is also used to map the input data into a high, dimensional feature space. This high dimensionality leads to a practical computational problem in feature space.

IV. Applications

Although biometric technologies are still in an early stage of development, it is possible to envisage a number of key application areas where they may be beneficial. Here some potential application areas are outlined. Biometric technologies may provide added robustness in access control to high security facilities within higher education. As the unit price for biometric devices continues to fall it is possible to employ these to replace the current systems used for workstation and network access. These devices are likely to become a standard computer peripheral, built into future workstations. A biometric system in its identification mode may be deployed to monitor surveillance cameras, and/or the telephone system within the campus. This will identify known specific individuals who may have been excluded from parts or from all of the facilities on campus. These could be known debtors, troublemakers etc. An experimental system similar to this has been developed to be in use for detecting known troublemakers [21]. In this mode the system will have been supplied with template information for specific individuals and will continuously search for a match with the faces and voices that it detects.

V. Conclusions

Biometric technologies are of significance in a range of security, access control and monitoring applications. The technologies are still new and rapidly evolving. A number of biometric modalities working together can result in increased performance, reliability and ease of use. There is therefore considerable interest in developing multimodal systems. The present paper has focused only on audio-visual biometrics. There is a need for investigating in more depth the range of other biometric technologies available and their potential applications. Additionally, there is a need for conducting more pilot projects to test the performance of some of the existing and future fusion technologies.

References

[1] Association for Biometrics and International Computer Security Association, “Glossary of Biometric Terms”, 1998.

[2] S G Davies, “Touching Big Brother – How biometric technology will fuse flesh and machine”, Information Technology and People, Vol. 7, No 4, 1994.

[3] B Millar, “Vital Signs of Identity”, IEEE Spectrum, pp 22-30, February 1994.

[4] C Jennings, “Biometrics – When the Person is the Key”, Sensor Review, Vol. 12, No. 3, pp 9-11, 1992.

[5] W Shen and R Khanna, “Scanning the Special Issue on Automated Biometrics”, Proceedings of IEEE, pp 1343-46, September 1997.

[6] European Union, “Directive on Data Protection”, Official Journal of the European Communities, No L. 281 p. 31, 23 November 1995.

[7] P Agre and M Rotenberg, eds., Technology and Privacy: The New Landscape, MIT Press, 1997.

[8] C C Chibelushi, F Deravi, J S D Mason, "Survey of Audio-Visual Speech Databases", Speech and Image Processing Research Group, Department of Electrical and Electronic Engineering, University of Wales Swansea, 1996.

[9] K Messer, J Matas, J Kittler, J Luettin, G Maitre, “XM2VTS: The Extended M2VTS Database”, Proceedings 2nd Conference on Audio and Video-based Biometric Person Authentication AVBPA’99, Springer Verlag, New York, 1999.

[10] C C Chibelushi, S Gandon, J S D Mason, F Deravi, R D Johnston, “Design Issues for a Digital Audio-Visual Integrated Database”, IEE Colloquium on Integrated Audio-Visual Processing for Recognition, Synthesis and Communication (London - UK), Digest No: 1996/213, pp. 7/1 - 7/7, 1996.

[11] C C Chibelushi, F Deravi, J S D Mason, “A Review of Speech-Based Bimodal Recognition – Part 1: Foundations for Audio-Visual Fusion by Machine” Submitted for Publication in IEEE Transactions on Multimedia, 1999.

[12] C C Chibelushi, F Deravi, J S D Mason, “A Review of Speech-Based Bimodal Recognition – Part 2: Techniques, Performance, and Challenges” Submitted for Publication in IEEE Transactions on Multimedia, 1999.

[13] J P Campell, “Speaker Recognition: A Tutorial”, Proceedings of the IEEE, Vol 85, No 9, pp 1437-1462, September 1997.

[14] H Wechsler, et al (Eds.) “Face Recognition From Theory to Applications”, NATO ASI Series. SERS. F, Springer-Verlag, Berlin/Heidelberg, 1998.

[15] A Samal, and P A Iyengar, “Automatic recognition and analysis of human faces and facial expressions: a survey”, Pattern Recognition, 25, 65-77, 1992.

[16] D Valentin, H Abdi, and G W Cottrell, “Connectionist models of face processing: A survey”. Pattern Recognition, 27, 1209, 1994.

[17] R B Starkey, “The Human Face – A Unique Pattern?” Sensor Review, Vol. 12, No. 3, pp 16-18, 1992.

[18] C C Chibelushi, J S D Mason and F Deravi, “Audio-Visual Person Recognition: An Evaluation of Data Fusion Strategies”, Proceedings of the European Conference on Security, IEE, London, pp 26-30, 28-30 April 1997.

[19] C C Chibelushi, J S D Mason and F Deravi, “Feature-level Data Fusion for Bimodal Person Recognition”, Sixth International Conference on Image Processing and its Applications, IEE, Trinity College, Dublin, Ireland, , pp 339-403, 14-17 July, 1997.

[20] C C. Chibelushi, F Deravi, J S D Mason, “Adaptive Classifier Integration for Robust Pattern Recognition”, Accepted for Publication, IEEE Transactions on Systems, Man and Cybernetics – Part B: Cybernetics, to appear December 1999.

[21] R A Wasniowski, Data Fusion for Biometrics authentication, RAW99-SR-320, 1999

[22] J D Woodward, “Biometrics: Privacy’s Foe or Privacy’s Friend?”, Proceedings of the IEEE, Vol. 85, No. 9, September 1997.

[23] M Willems and P Forret, “Layered Biometric Verification”, Keyware Technologies, 1997

[24] P K Varshney, “Multisensor Data Fusion”, Electronics and Communications Engineering Journal