RESEARCH ISSUES IN INFORMATION FUSION FOR MULTIMODAL BIOMETRICS

Sukhdev Singh and Vinay Goyal

Department of Computer Science, D.A.V. College (Lahore), Ambala City

ABSTRACT

Information fusion refers to integrate different information originated from different sources.It is one of the main factors of designing a biometric system involving more than one biometric source. In this paper, various information fusion techniques in the context of multimodal biometric systems are discussed. Usually, the information in a multimodal biometric system can be combined in senor level, feature extraction level, match score level, rank level, and decision level. Another popular fusion method is—the fuzzy fusion. Fuzzy fusion deals with the quality of the inputs or with the quality of any system components. This paper discusses the associated research challenges related to making the choice of appropriate fusion method for the application domain, to balance between fully automated versus user defined operational parameters of the system and to take the decision on governing rules and weight assignment for fuzzy fusion.

Keywords: biometric, fusion, multimodal and information.

Introduction

Biometric system have different properties: distinctiveness, universality, permanence, acceptability, collectability, and security. As per literature study of biometric system, no existing biometric security system simultaneously meets all of these requirements. Despite it multibiometric provide tremendous progress in this field than unimodal biometric trait. Unimmodal biometric not always provide satisfy result, the combination of traits from different biometrics gives better result [1].

Thus, Multimodal biometrics appear as a new and highly promising approach to biometric knowledge representation, which seek to overcome thelimitations of unimodal biometric matchers by combining the information presented by multiple biometric traits [2]. As an example, a multimodal system may use both ear, face recognition and finger print to authenticate a person. Due to reliable and efficient security solutions in the security critical applications, multimodal biometric systems have evolved over last decade as a feasible alternative to the traditional unimodal biometric security systems

1.1 Benefit Of Multimodal Biometric System

The benefit of multimodal biometric systems over unimodal biometric systems are mainly due to utilization of more than one information source or trait. A sample of multimodal biometric system has shown in figure 1. The most outstanding implications of this are increased and reliable identification performance, fewer registration problems, and enhanced the biometric system security [3].

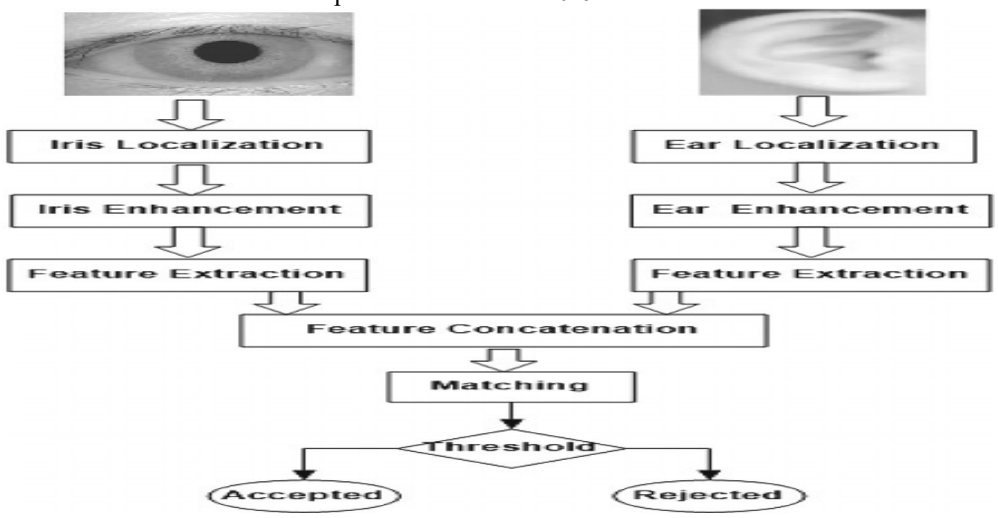

Figure 1. A sample multibiometric system architecture [3].

1.2 Enhanced and Reliable Identification Performance

A multimodal system permits for a greater level of certainty of a proper match in identification modes and verification[4]. As multimodal biometric systems use more than one biometric trait, each of those traits can offer additional information about the legitimacy of any identity claim. For example, the gaits of two persons of the same family can be similar. In this premise, a unimodal biometric system based only on gait pattern analysis may results in false recognition. If the same biometric system also includes face matching, the system would results in increased identification rate, as it is very unlikely that two different persons have same gait and face patterns.

Another example of enhanced and reliable identification performance of multimodal biometric systems is ability to effectively handle the noisy or poor quality data. When the biometric information inherit from a single biometric trait is not reliable due to noise, the availability of other biometric trait allows the system to still perform in a secure manner. For example, in a face and voice-based multimodal biometric system, due to noise, if the individual's voice signals cannot be accurately measured, the facial characteristics may be used for authentication.

1.3 Fewer Registration Problems

Multimodal biometric systems solve the problem of non-universality or insufficient population coverage, in which part of the population has a biometric feature that is missing or unrecognizable, and thus significantly reduces the failure rate in the population. Depending on the system design, many multimodal biometric systems can perform pairing even in the absence of one of the biometric samples. For example, in a multimodal system based on fingerprints and a face, a person (who is a carpenter) cannot enter fingerprint information into the system due to scars on the fingerprint. In this case, the multimodal system can still authenticate using that person's facial features. Also, if some fingerprint functions can be extracted (but not all due to finger damage), you can still require these functions to increase the accuracy index or confidence level of the final decision.

1.4 Enhanced Security

Multimodal biometric systems make it difficult for the fraudster to falsify biometric features of a legally registered person. A parody attack occurs when a person pretends to be someone else, using stolen identification data or false information. For example, scientists have shown how to create fake fingerprints, which has been somewhat successful in avoiding the commercial security of the fingerprint recognition system [5]. The advantage of multimodal systems is that the fraudster would have to fake more than one biometric feature at the same time, which would be much more difficult. Multimodal biometric systems can also serve as a fault-tolerant system. For example, multimodal systems can still perform their functions and obtain relatively reliable results, even when some biometric modules stop working (due to sensor malfunction, software problems, lack of availability of sample data or extremely low quality). The more high-quality data received, the better the overall accuracy indicators of the multibiometric system.

2. Developmental Issues Of Multibiometric Systems

Developing a multibiometric system for security reasons is not an easy task. As with any unimodal system, the data acquisition procedure, information sources, expected level of accuracy, system reliability, user training, data privacy and dependence on the proper functioning of the equipment and proper operating procedures directly affect the performance of the security system. Although the use of more than one data source alleviates some problems (such as noisy data, missing samples, acquisition errors, forgery, etc.), this advantage is not free. The biometric information must be selected, which must be integrated or combined, the information synthesis methodology must be chosen, the cost-benefit analysis must be performed, processing sequences must be developed and system operators must be trained [6].

2.1. Ease of Data Acquisition Procedure

One of the key design issues of a multibiometric security system is a convenient interface with the system to ensure the effective acquisition of biometric information. As indicated in Jain [7]: appropriate An appropriately designed interface can ensure that a large amount of evidence regarding a person's identity is obtained reliably, causing minimal inconvenience to the user. For example, in a multimodal biometric system based on the face, ear and fingerprints, if the user has to present their three biometric identifiers separately, it would be very inconvenient. On the other hand, if three biometric identifiers can be obtained simultaneously (or in one place), it may be more convenient that biometric identifiers (or in one place) can be obtained simultaneously, which may be more convenient for the user. Unfortunately, so far there has been very little research on this aspect of human-computer interaction with the biometric system.

2.2Source of Information

Multibiometric systems depend on more than one source of biometric information. Much biometric information can come from multiple identifiers, from individual identifiers, but with multiple samples or instances, or from a combination of both. The sources of biometric information in such systems depend on several problems, including the need and application scenarios, the availability of biometric information, the costs associated with the process of obtaining biometric information, the choice of algorithms to match patterns and the synthesis of information.

2.3Choice of Biometric Information

The integration of biometric information or fusion can occur at various levels, from the initial stage after obtaining raw data to the final stage after obtaining the final decision on pairing / non-pairing. Then, the extracted functions, the matching results or the final classification list, all of them can be integrated with a multibiometric system. The information to be combined is one of the key decisions regarding the design of a multibiometric system [8]. Integration generally depends on the application scenario and the availability of information. For example, in some multibiometric systems (especially commercial biometric security systems) only the final decision is available. In this case, only the fusion of decision making is possible for this multibiometric system.

Information Fusion Methodology

For all types of information synthesis in multibiometric systems, there are several alternative algorithms that can be used [8]. For example, to obtain consensus ranking lists, initial ranking lists (obtained after matching input data and templates) can be integrated using the highest ranking method, the Bord count method, the method of Logistic regression, the Bayes method, the diffuse method or the Markov chain method. The approach to be used depends on the designer of the system, the results of the previous methodology and the resistance of the system required.

3.1Cost vs. Benefits

One of the disadvantages of developing a multibiometric system is the higher cost compared to a single biometrics-based security system. Then, before deciding on a multimodal biometric approach, it is necessary to analyze the potential benefits that can be obtained by developing a multibiometric system. The cost depends on the number of sensors installed, the time required to obtain biometric data, the experience of the user or operator of the system and the maintenance of the system [9].

3.2. Processing Sequences

Another important issue in the design of a multibiometric system is the method of data acquisition or processing in the system [10]. In the case of simultaneous data acquisition or processing or parallel data acquisition or processing, a decision must be made in advance. Usually, there are two possible ways to choose the sequence of data acquisition. In the process of serial data acquisition, multibiometric data is collected sequentially in a short period of time. In a

parallel data acquisition process, all multibiometric data is collected in parallel, which makes the system faster than the sequential method.

In the data processing stage in any multibiometric system, you can use parallel or cascade mode. In cascade mode, the processing of biometric data takes place sequentially, while in the parallel processing of biometric data, all biometric data is processed simultaneously and used in the authentication process.

Figure 3.1 illustrates the cascade processing sequence, and Figure 3.2 illustrates the parallel processing sequences for a multi-biometric security system.

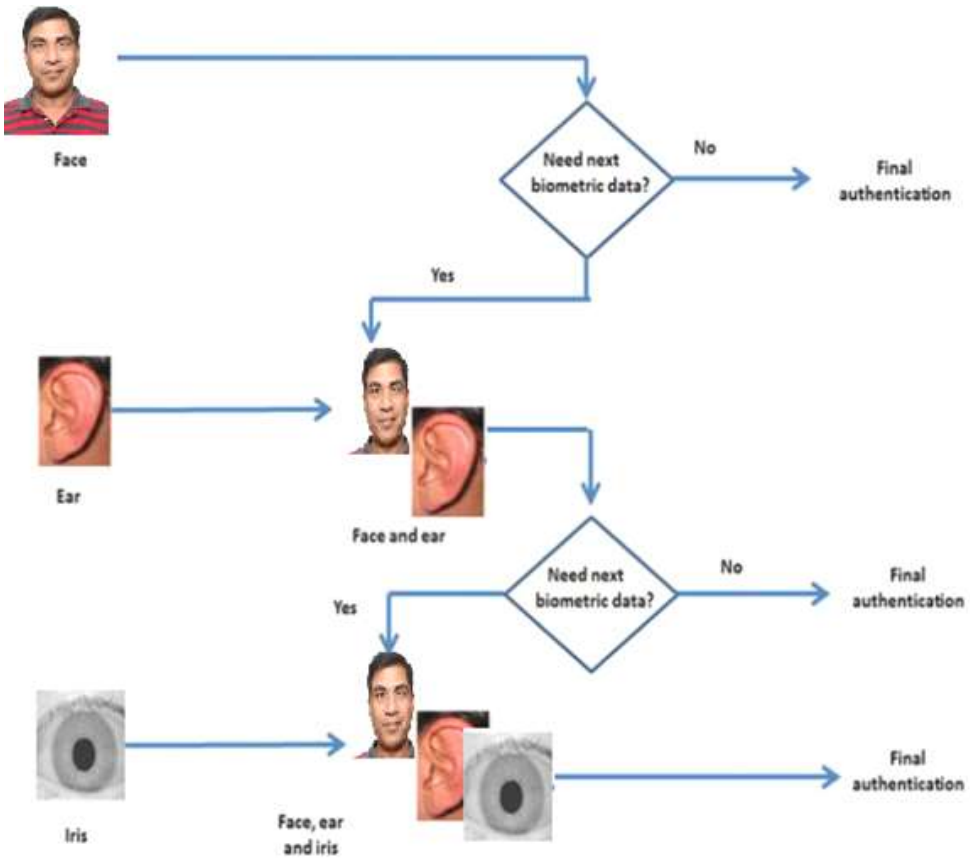

Figure 3.1. Multimodal biometric data processing sequence: cascade mode [12]

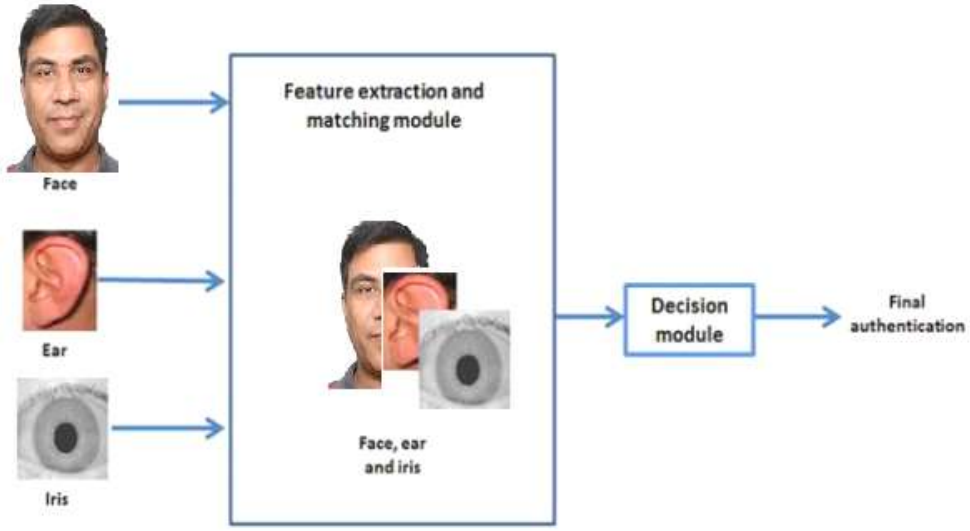

Figure 3.2 Multimodal biometric data processing sequence: parallel mode [12]

Information Sources For Multibiometric Systems

It should be noted that there is a slight difference between the two terms in the literature. The term multimodal biometric system refers in particular to those biometric systems that use more than one biometric modality. The term multibiometric is more general and includes multimodal systems and some other configurations that use only a biometric modality with different sample instances or algorithms. Multiple sensors: a biometric characteristic: these systems use different sensors to capture different representations of the same biometric modality to extract different information [13]. For example, a biometric system can use 2D, 3D or thermal facial images for authentication. Because these systems include only one biometric characteristic, if a particular biometric characteristic is unavailable or inappropriate, the benefits of many acquisitions will be minimal.

Multiple instances: a biometric feature: in these systems, multiple instances of the same biometric feature are used for authentication. For example, the image of the patient's left and right eyes can be used in the retinal recognition system. These systems are cost effective because you can use the same sensors or the same extraction and matching algorithm.

Many algorithms: a biometric characteristic: these systems use a biometric characteristic, but use different matching algorithms. For example, the system can use its own face and Voronoi diagram as matching algorithms for the same set of face images, and then combine the results. These systems also suffer from poor input quality.

Multiple samples with a sensor: a biometric characteristic: these systems use a sensor, but many samples of the same biometric characteristic for authentication. For example, a single sensor can be used to capture different facial images of a person, and then a mosaic pattern can be used to construct a facial image composed of all available facial images of that object.

Many biometric features: these systems use more than one biometric feature and, therefore, are called multimodal systems. For example, a biometric system can use face and voice to authenticate a person. The cost of implementing these systems is much higher due to the requirements of new sensors and the development of a new user interface [9]. Identification accuracy can be improved using an increasing number of features. These systems also maximize

the independence between biometric samples and, therefore, the low quality of the biometric function does not affect authentication with another function.

Multiple tokens: this is a typical authentication system consisting of one or more biometric identifiers and a possession or knowledge token [9]. The possession and knowledge token can be, for example, an identity document and a password.

Hybrid systems: these systems use more than one scenario discussed above for reliable authentication [14]. For example, the biometric system can use two iris matching algorithms and three face matching algorithms in the same iris and biometric iris multimodal system. The ideas of hybrid algorithms in biometrics are not new. They were successfully used in unique biometric recognition systems, when methods based on appearance and topology were used to improve recognition. For example, the fingerprint recognition system based on the Voronoi diagram is based on both geometric properties (such as triangle edge length) and topological properties (comparison of the spine pattern) when making the final decision of recognition.

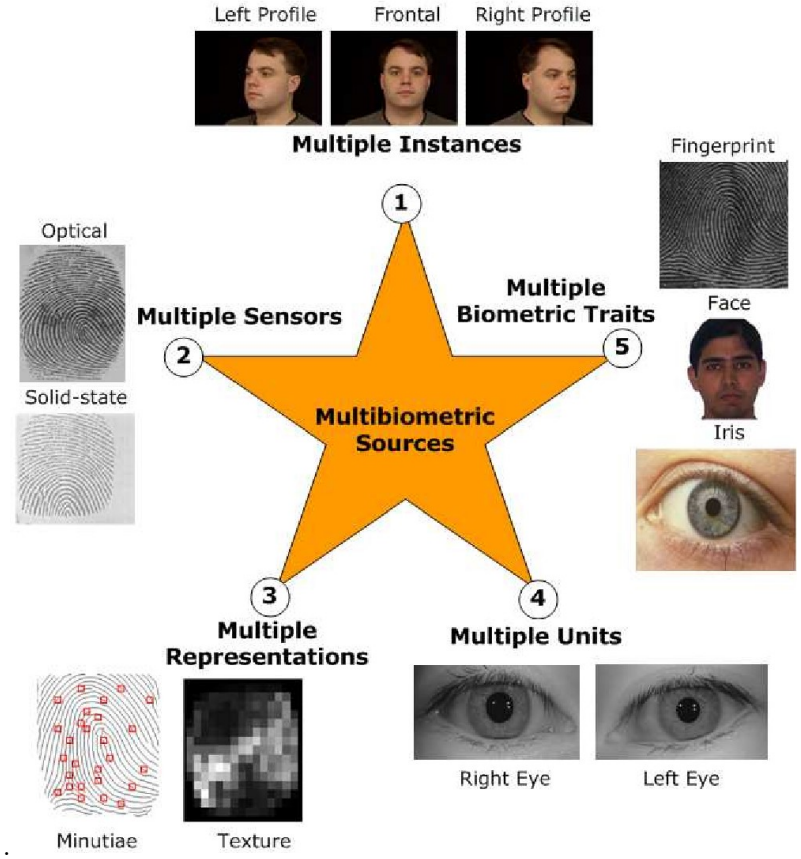

Figure 4.1 Possible information sources of multibiometric systems

V. Conclusion

In general, information from various sources in a multimodal biometric system can be combined at the sensor level, feature extraction level, match result level, range level and decision level. Of all the methods of synthesis, the synthesis of the sensor and the synthesis of the level of extraction of characteristics are considered the stage of combining raw data or real biometric data. The combination of results, range and decision level methods combine processed data or data obtained as a result of some experiments. There is also another novel fusion method that is becoming very popular: diffuse fusion

There are many challenges in this area that require further study. The first is based on the selection of the most appropriate fusion method for the field of application. The decision is often made ad-hoc or based on insignificant restrictions, such as the availability of the welding module, low cost, etc., and is not based on the actual match of the application area and method.

The second challenge is a balance between fully automated and user-defined system operating parameters. Although complete automation may be a desirable function for large applications that require large scale, in practice this is not always possible or desirable. The best way to develop a biometric security system is to design it as a decision support system that can provide the system operator with information that allows him to make an intelligent and correct decision.

REFERENCE

1. Aarabi, P., &Dasarathy, B. V. (2014). Robust speech processing using multi-sensor multi-source information fusion: An overview of the state of the art. Information Fusion , 5, 77–80.
2. [2]. Abaza, A., &Ross, A. (2012). Quality based rank-level fusion in multibiometric systems. In *Proceedings of 3rd IEEE International Conference on Biometrics: Theory, Applications andSystems*. Washington, DC: IEEE.
3. Ailon, N.,Charikar, M., & Newman, A. (2015). Aggregating inconsistent information: Ranking and clustering. In *Proceedings of 37th Annual ACM Symposium on Theory of Computing (STOC)*, (pp. 684-[11]. Tumer, K., & Gosh, J. (2009). Linear order statistics combiners for pattern classification .
4. In Proceedings of Combining Artificial Neural Networks (pp. 127–162). IEEE
5. Bailly-Baillire, E., Bengio, S., Bimbot, F., Hamouz, M., Kittler, J., &Marithoz, J. Thiran, J. P. (2013). The BANCA database and evaluation protocol. In *Proceedings of International Conference on Audio-and Video-Based Biometric Person Authentication*, (pp. 625-638). Guildford, UK: IEEE.
6. Benitez, A. B., & Chang, S. F. (2012). Multimedia knowledge integration, summarization and evaluation. In *Proceedings of Workshop on Multimedia Data Mining*, (vol. 2326). Springer.
7. Jain, A. K., Hong, L., &Bolle, R. (2010). On-line fingerprint verification. IEEE Transactions on Pattern Analysis and Machine Intelligence , 19(4), 302–314. doi:10.1109/34.587996
8. Jain, A. K.,Nandakumar, K., & Ross, A. (2015). Score normalization in multimodal biometric systems.PatternRecognition , 38, 2270–2285. doi:10.1016/j.patcog.2005.01.012
9. Jing, X. Y., Yao, Y. F., Yang, J. Y., Li, M., & Zhang, D. (2016). Face and palmprint pixel level fusion and kernel DCV-RBF classifier for small sample biometric recognition. Pattern Recognition , 40, 3209–3224. doi:10.1016/j.patcog.2007.01.034
10. Kludas, J., Bruno, E., &Marchand-Maillet, S. (2011). Information fusion in multimedia information retrieval. Lecture Notes in Computer Science , 4918, 147–159. doi:10.1007/978-3-540-79860-6_12
11. Kokar, M. M., Weyman, J., &Tomasik, J. A. (2014). Formalizing classes of information fusion systems.InformationFusion , 5, 189–202. doi:10.1016/j.inffus.2003.11.001