American Journal of Engineering Research (AJER) ***2017***
American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-4, pp-148-154
www.ajer.org
Research Paper Open Access

Current Practices in Information Fusion for Multimodal Biometrics

[1]Oloyede Ayodele and [2]Aderonke Adegbenjo
[1] *Department of Computer Science, Caleb University, Imota, Lagos State*
[2] *Department of Computer Science & Information Technology, Babcock University, Ilishan-Remo, Ogun State*

ABSTRACT
Integrating different information originating from different sources, known as information fusion, 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. There is also another emerging fusion method, which is becoming popular—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 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: Biometrics, Fusion, Multimodal and Information.

I. Introduction

The optimal biometric system is one having the properties of distinctiveness, universality, permanence, acceptability, collectability, and security. As we saw in the introductory papers, no existing biometric security system simultaneously meets all of these requirements. Despite tremendous progress in the field, over the last decades researchers noticed that while a single biometric trait might not always satisfy secure system requirements, the combination of traits from different biometrics will do the job. The key is in aggregation of data and intelligent decision making based on responses received from individual (unimodal) biometric systems.(Aarabi, et al, 2014).
Thus, Multimodal biometrics emerged as a new and highly promising approach to biometric knowledge representation, which strives to overcome problems of individual biometric matchers by consolidating the evidence presented by multiple biometric traits (Abaza,, 2012). As an example, a multimodal system may use both face recognition and signature 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 viable alternative to the traditional unimodal security systems

1.1 ADVANTAGES OF MULTIMODAL BIOMETRIC SYSTEM

The advantages of multimodal biometric systems over unimodal systems are mainly due to utilization of more than one information source. Figure 1 shows a sample multimodal biometric system. The most prominent implications of this are increased and reliable recognition performance, fewer enrolment problems, and enhanced security (Ailon, 2015).

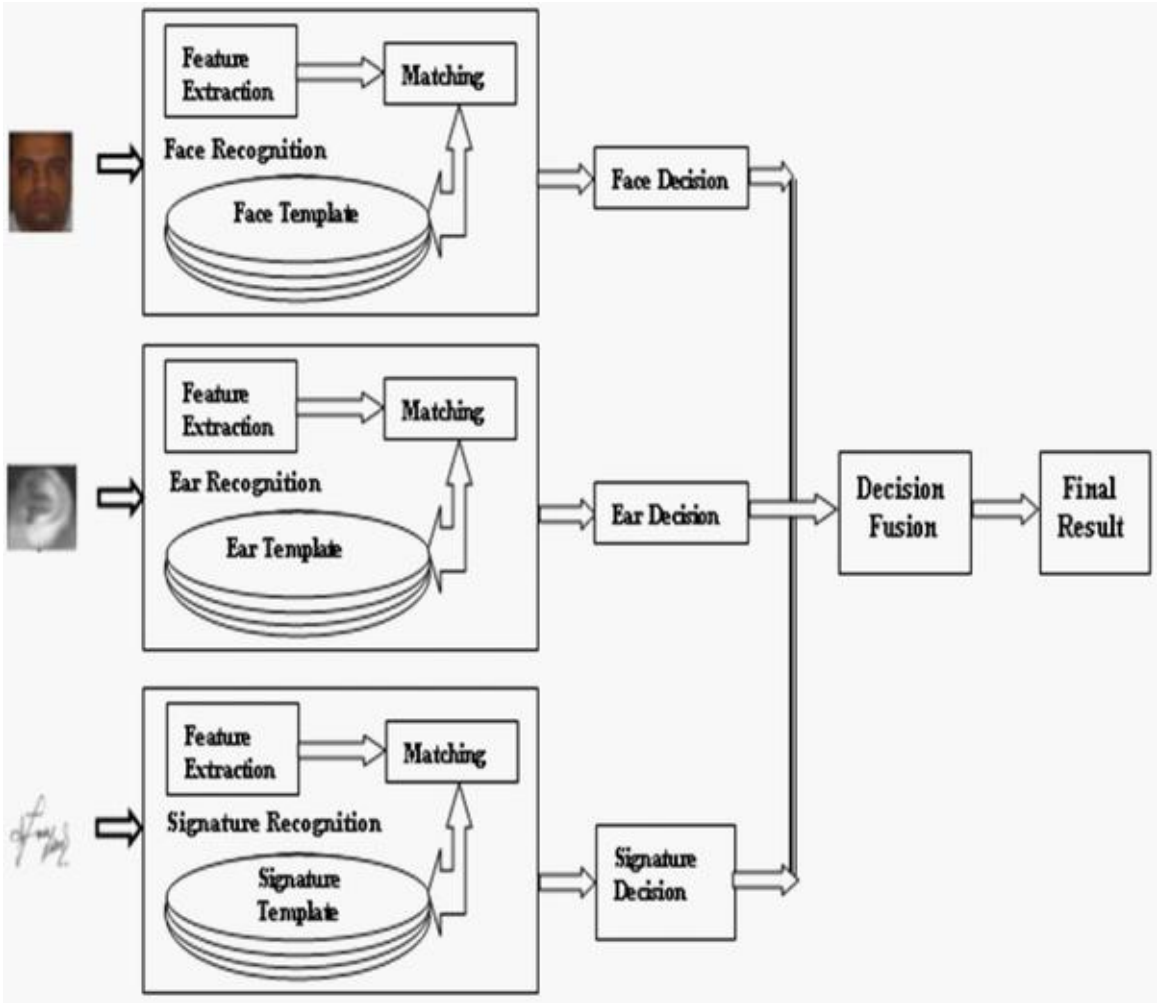

Figure 1. A sample multibiometric system architecture (Ailon, 2015).

1.2 Increased and Reliable Recognition Performance

A multimodal system allows for a greater level of assurance of a proper match in verification and identification modes (Bailly-Baillire, 2013). As multimodal biometric systems use more than one biometric trait, each of those traits can offer additional evidence about the authenticity of any identity claim. For example, the gaits (the patterns of movements) of two persons of the same family (or coincidentally of two different persons) can be similar. In this scenario, a unimodal biometric system based only on gait pattern analysis may results in false recognition. If the same biometric system also includes fingerprint matching, the system would results in increased recognition rate, as it is very unlikely that two different persons have same gait and fingerprint patterns.

Another example of increased and reliable recognition performance of multimodal biometric systems is ability to effectively handle the noisy or poor quality data. When the biometric information acquired from a single trait is not reliable due to noise, the availability of other 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 Enrolment Problems

Multimodal biometric systems address the problem of non-universality or the insufficient population coverage, where a portion of a population has a biometric characteristic that is missing or not suitable for recognition, and thus reduce the failure to enroll rate significantly (Frischholz & Dieckmann, 2000). Depending on the system design, many multimodal biometric systems can perform matching even in the absence of one of the biometric samples. For example, in a fingerprint and face based multimodal system, a person (who is a carpenter) cannot enroll his fingerprint information to the system due to the scars in his fingerprint. In this case, the multimodal system can still perform authentication using the facial characteristics of that person. Moreover, if certain features can be extracted from fingerprint (but not all due to damage to the finger), then these features still can be sued to increase accuracy rate or confidence level of the final decision.

2.4 Enhanced Security

Multimodal biometric systems make it more difficult for an impostor to spoof biometric traits of a legitimately enrolled individual. A spoof attack is where a person pretends to be another person by using stolen ID or falsified information. For example, researchers have demonstrated how to create fake fingerprints, which had some success in bypassing commercial fingerprint recognition system security (Matsumoto, Matsumoto, Yamada, &Benitez, 2012). The advantage of multimodal systems is that the impostor would need to spoof more than one biometric trait simultaneously, which would be significantly more challenging. Multimodal biometric systems can also serve as a fault tolerant system. For example, multimodal systems can still perform their functions and result in relatively reliable outcomes even when certain biometric modules stop operating (due to sensor malfunction, software issues, unavailability of a sample data or quality being extremely low). The more high quality data is received, however, the better overall multibiometric system accuracy rates would normally become.

II. Developmental Issues Of Multibiometric Systems

Development of a multibiometric system for security purposes is not a trivial task. As with any unimodal system, the data acquisition procedure, sources of information, level of expected accuracy, system robustness, user training, data privacy, and dependency on proper functioning of hardware and proper operational procedures impact directly the performance of security system. While using more than one data source alleviates some issues (such as noisy data, missing samples, errors in acquisition, spoofing etc.), this advantage does not come free. The choice of biometric information that needs to be integrated or fused must be made, information fusion methodology should be selected, cost vs. benefit analysis needs to be performed, processing sequences developed, and system operators trained (Jain et al, 2010).

2.1. Ease of Data Acquisition Procedure

One of the key design issues of a multibiometric based security system is a convenient interface with the system to ensure the efficient acquisition of biometric information. As stated in Jain (2015): "An appropriately designed interface can ensure that multiple pieces of evidence pertaining to an individual's identity are reliably acquired whilst causing minimum inconvenience to the user". For example, in a face, ear and fingerprint based multimodal biometric system, if a user needs to present his/her three biometric identifiers separately, that would be very inconvenient. Instead, if the three biometric identifiers can be acquired simultaneously (or in one seating), that might be more convenientbiometric identifiers can be acquired simultaneously (or in one seating), that might be more convenient for user. Unfortunately, up to date, there have been too few studies looking into this aspect of human-computer interaction with the biometric system.

2.2 Source of Information

Multibiometric systems are based on more than one biometric information source. Multiple biometric information can be derived from multiple identifiers, from single identifiers but with multiple samples or instances, or from a combination of both (Ross, Nandukamar, & Jain, 2006). The sources of biometric information in such systems depend on a variety of issues including the application necessity and scenarios, the availability of the biometric information, the cost associated with the biometric information acquisition process, the choice of pattern matching and information fusion algorithms.

2.3 Choice of Biometric Information

Biometric information integration (or fusion) can occur in various levels, from the initial stage after acquiring the raw data to the final stage after obtaining the final match/non-match decision. Next, the extracted features, the matching scores or the final ranked list—all of these can be integrated in a multibiometric system. Which information needs to be fused is one of the crucial decisions of a multibiometric system design (Jing, 2016). The integration usually depends on the application scenario and on the availability of information. For example, in some multibiometric systems (specially, in commercial biometric security systems) only the final decision is available. In this case, only the decision fusion is possible for that multibiometric system.

III. Information Fusion Methodology

For all types of information fusion in multibiometric systems, there are several alternative algorithms that can be used (Jing, 2016). For example, to get the consensus ranked lists, the initial ranked lists (obtained after matching input and templates) can be integrated by the highest rank method, Borda count method, logistic regression method, Bayesian method, fuzzy method, or Markov chain method. What approach needs to be taken depends on the designer of the system, previous performances of the methodologies and the robustness required for the system.

3.1 Cost vs. Benefits

One of the drawbacks of multibiometric system development is the higher cost, as compared to a single biometric based security system. So, before making commitment to multimodal biometric approach, analyzing the potential benefits that can be obtained through the development of multibiometric system is necessary. The cost depends on the number of sensors deployed, the time it takes to acquire biometric data, user or system operator experience, and system maintenance (Kludas, 2011)

3.2. Processing Sequences

Another important issue in multibiometric system design is how the acquisition or data processing will occur for the system (Kokar, 2014). Should the data be acquired or processed simultaneously, or should the data be acquired or processed in parallel must be decided in advance. Usually, there are two possible ways to choose the data acquisition sequences. In serial data acquisition process, the multibiometric data is acquired sequentially and within a short time interval. In the parallel data acquisition process, all the multibiometric data is gathered in parallel which makes the system faster than sequential method.

In the data processing stage, parallel or cascade mode can be used in any multibiometric system. In the cascade mode, the processing of biometric data occurs sequentially, while in parallel biometric data processing, all biometric data is processed simultaneously and used in authentication process (Tumer, 2009).

Figure 3.1 illustrates cascade processing sequence and Figure 3.2 illustrates parallel processing sequences for multibiometric security system.

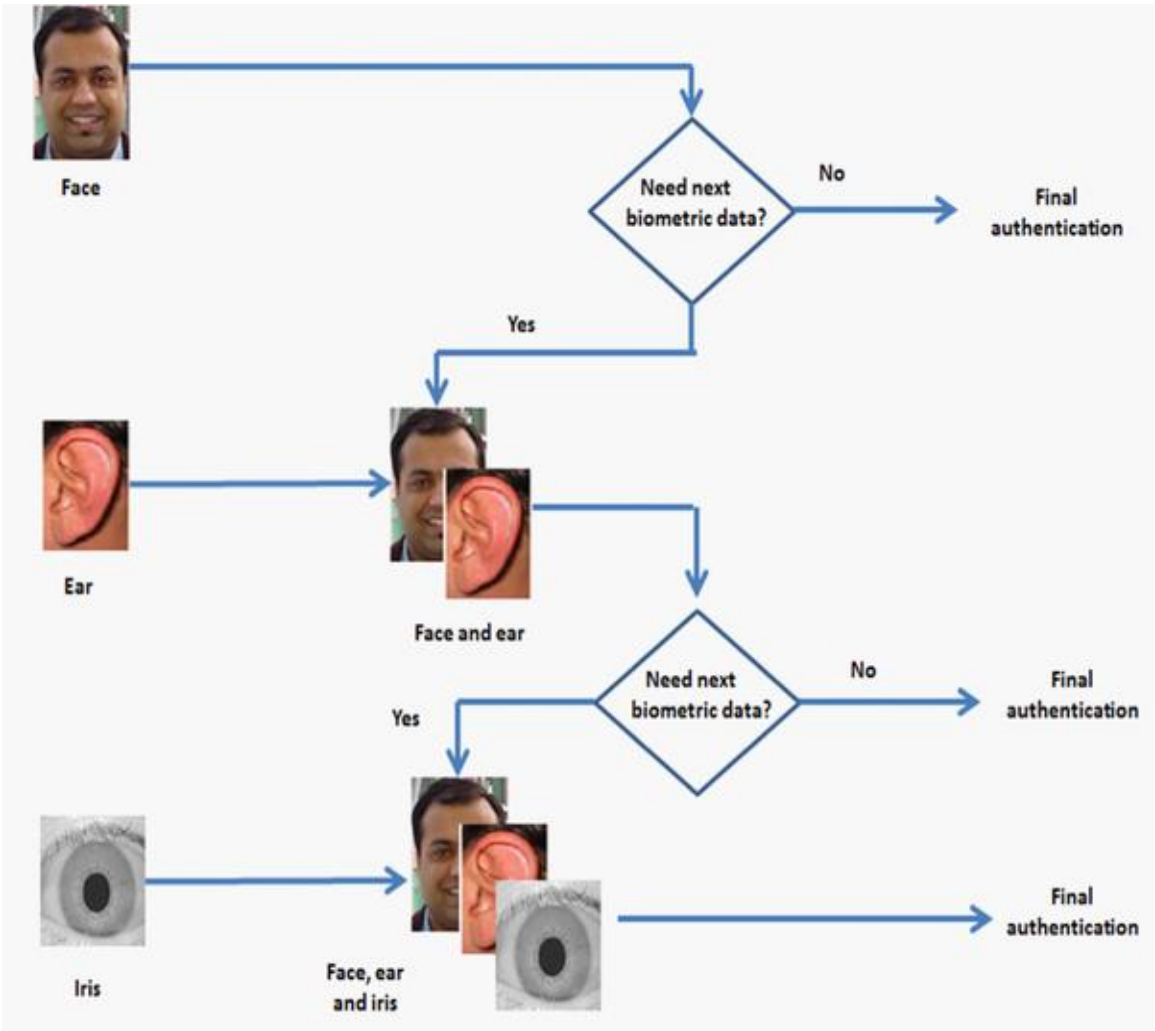

Figure 3.1. Multimodal biometric data processing sequence: cascade mode (Wang, 2015)

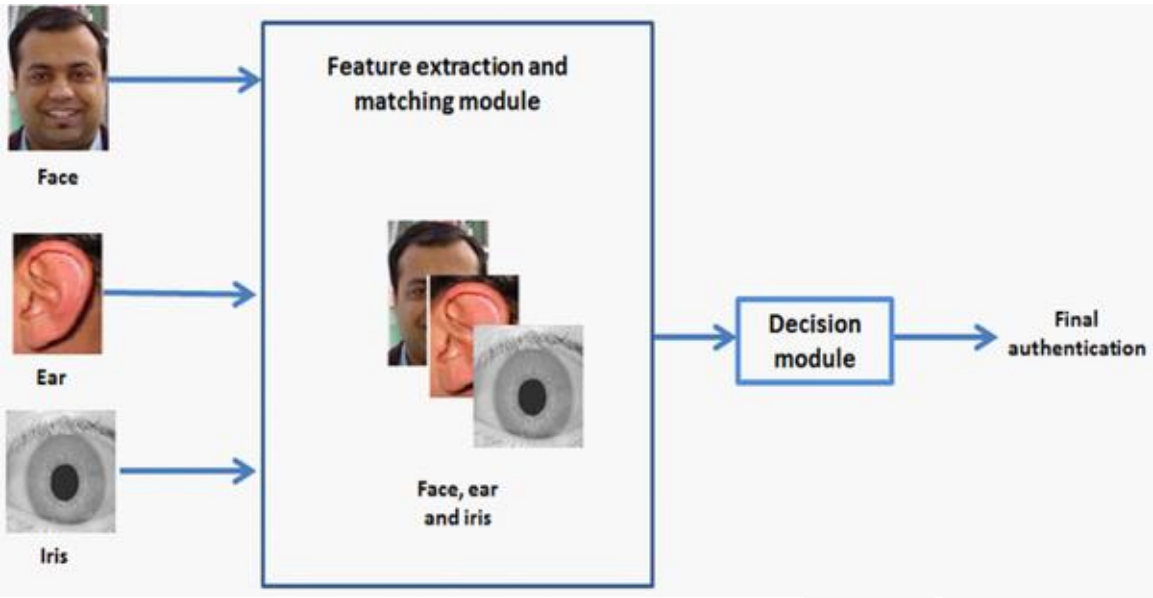

Figure 3.2 Multimodal biometric data processing sequence: parallel mode (Wang, 2009)

IV. Information Sources For Multibiometric Systems

It must be pointed out that in literature there is a slight difference between two terms. The term *multimodal* biometric system refers specifically to those biometric systems where more than one biometric modalities are used (Wang, 2012). The term *multibiometric* is more generic and includes multimodal systems and some other configurations using only one biometric modality with different samples instances or algorithms.

Multiple Sensors - One Biometric Trait: In these systems, different sensors are used for capturing different representations of the same biometric modality to extract diverse information (Wang, 2012). For example, a biometric system may use 2D, 3D, or thermal face image for authentication. As these systems consider only one biometric trait, so if the specific biometric trait is missing or not suitable, the performance benefits of multiple acquisitions will be minimal.

Multiple Instances - One Biometric Trait: In these systems, multiple instances of the same biometric trait are used for authentication (Wang, 2012). For example, the image of left and right eye of a subject may be used for retina recognition system. These systems are cost efficient, as thesame sensors or the same feature extraction and matching algorithm can be used.

Multiple Algorithms – One Biometric Trait: These systems use one biometric trait but use different matching algorithms (Wang, 2012). For example, a system may use eigenface and Voronoi diagram as matching algorithms for the same set of face images and later combine the results. These systems also suffer with the poor quality of input.

Multiple Samples with Single Sensor– One Biometric Trait: These systems use single senor but multiple samples of the same biometric trait for authentication (Wang, 2012). For example, a single sensor may be used to capture different facial expression images of a subject and latter a mosaic scheme may be used to build a composite face image from all the available face images of that subject.

Multiple Biometric Traits: These systems use more than one biometric trait and hence are referred to as multimodal systems. For example, a biometric system may use face and voice for person authentication. The cost of deploying these systems is substantially more due to the requirements of new sensors and for the development of the new user interface (Kludas, 2011). The identification accuracy can be improved by utilizing an increasing number of traits. These systems also maximize the independence between the biometric samples, and hence the poor quality of a biometric trait has no impact on the authentication with other trait.

Multiple Tokens: This is the typical authentication system consists of one or more biometric identifiers as well as a possession or knowledge token (Kludas2011). The possession and knowledge token can be ID card and password, for example.

Hybrid Systems: These systems use more than one scenarios discussed above for robust authentication (Ailon, 2015). For example, a biometric system may use two iris matching algorithms and three face matching algorithms in the same face and iris based multimodal biometric system. The ideas of hybrid algorithms in biometrics are not new. They were successfully used in single biometric recognition systems, when both appearance-based and topology-based methods were used for enhanced recognition. As example, the fingerprint recognition system based on Voronoi diagram relies both on geometric properties (such as triangle edge length) and topological properties (ridge pattern comparison) in making final recognition decision (Benitez, 2012).

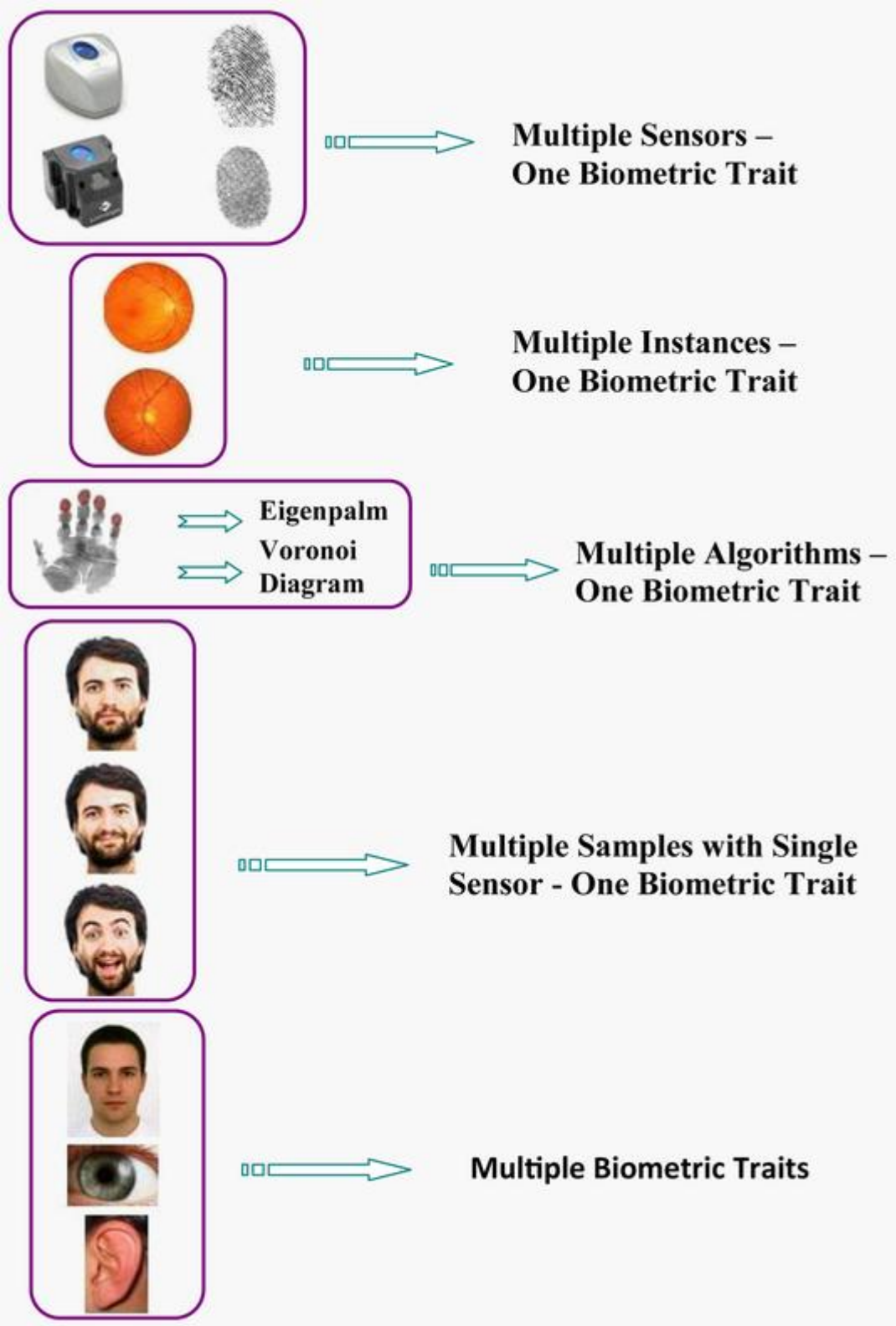

Figure 4.1 Possible information sources of multibiometric systems

V. Conclusion

Usually, the information originated from different sources in a multimodal biometric system can be combined in senor level, feature extraction level, match score level, rank level, and decision level. Among all of the fusion methods, senor fusion and feature extraction level fusion considered as the stage for combining raw data or the

actual biometric data. Match score, rank and decision level fusion methods combine processed data or data obtained through some experimentations. There is also another novel fusion method which is becoming highly popular: the fuzzy fusion.

There are a number of challenges in this area, requiring further investigation. The first one is rooted in the choice of a fusion method, most appropriate for the application domain. The decision is often made ad-hoc, or based on non-essential constraints such as availability of the fusion module, low cost, etc, instead of being made based on actual fit of the application area and the method.

The second challenge lies in the balance between fully automated vs user defined operational parameters of the system. While complete automation might be a desired feature for some high0-demand large-scale applications, 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,* which can provide information to the system operator empowering 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. doi:10.1016/j.inffus.2004.02.001

[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 and Systems*. 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. 684-693). Baltimore, MD: ACM.

[4]. 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.

[5]. Benitez, A. B., & Chang, S. F. (2012). Multimedia knowledge integration, summarization and evaluation. In *Proceedings of Workshop on Multimedia Data Mining*, (vol. 2326). Springer.

[6]. 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

[7]. 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

[8]. 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

[9]. 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

[10]. 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

[11]. Tumer, K., & Gosh, J. (2009). Linear order statistics combiners for pattern classification . In Proceedings of Combining Artificial Neural Networks (pp. 127–162). IEEE.

[12]. Wang, C., & Gavrilova, M. (2015). A novel topology-based matching algorithm for fingerprint recognition in the presence of elastic distortions. In *Proceedings of International Conference on Computational Science and its Applications*, (vol. 1, pp. 748-757). Springer.

[13]. Wang, Y. (2009). Toward a formal knowledge system theory and its cognitive informatics foundations. Transactions of Computational Science , 5, 1–19.

[14]. Wang, Y.-P., Dang, J.-W., Li, Q., & Li, S. (2012). Multimodal medical image fusion using fuzzy radial basis function neural networks. In *Proceedings International Conference on Wavelet Analysis and Pattern Recognition*, (vol. 2, pp. 778-782). Beijing, China: IEEE.