Biometric Importance and Security in Modern Society

Surender Kumar[1], Dr. Rajan Manro[2]

1. Research Scholar, Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh (Punjab).
2. Research Guide, Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh (Punjab).

Abstract

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification systems. As the level of security infringes, the requirement for highly secure identification and personal verification technologies are becoming apparent. When adopting a biometric technology for identification, the most important question is whether to choose a unimodal(which use a single biometric trait of the individual for identification and verification) or multimodal(which use or are capable of using a combination of two or more biometric modalities to identify an individual) biometric system. This paper discusses both these systems, the limitations of unimodal biometric systems and how these limitations are overcome by the use of multimodal biometric systems.

Keywords: Biometrics identification, unimodal system, multimodal system.

1.Introduction

Biometrics is automated method of recognizing a person based on a physiological or behavioral characteristic. Biometrics technology is based on the principle of measuring and examining the biological traits of individuals, extracting the unique features from this acquired data and then comparing it with the template set stored in the biometric templates database. These unique biological traits are called biometric identifiers and can be of two types – physiological and behavioural. The physiological identifiers are related to the shape of the body whereas the behavioural identifiers are related to the behavioural patterns of individuals. Physiological biometric identifiers include fingerprints, face, iris, palm, hand geometry etc. whereas behavioural identifiers include such characteristics as gait, voice, typing rhythm etc[1]. Since, today, a large number of applications require reliable verification methods to confirm the identity of an individual, recognizing humans based on their body characteristics, Biometrics became more and more popular in emerging technologies[2].The necessity for biometrics can be found in, state and local governments, federal, in the military, and in commercial applications. Enterprise wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies[3].

2. Biometrics System

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses[4].A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

Identification (1: n) One-to-Many: Biometrics can be used to determine a person's identity even without his awareness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database.

Verification (1:1) One-to-One: Biometrics can also be used to verify a person's identity. Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan[5].

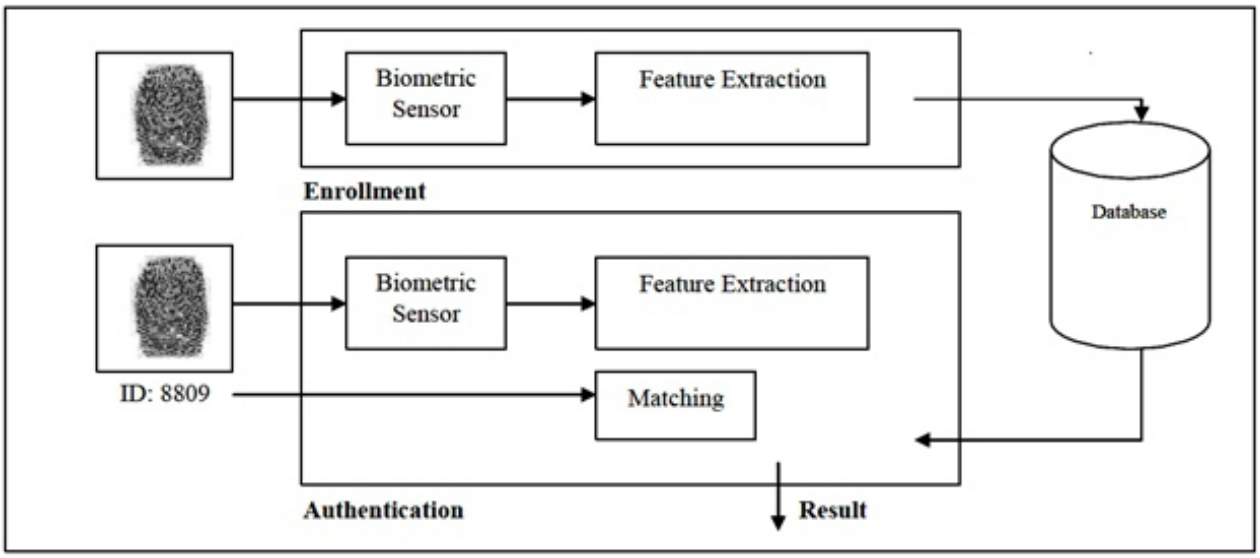

Figure 1: General Biometric System

A simple biometric system consists of four basic components:
1) Sensor module which acquires the biometric data.
2) Feature extraction module where the acquired data is processed to extract feature vectors
3) Matching module where feature vectors are compared against those in the template.
4) Decision-making module in which the user's identity is established or a claimed identity is accepted or rejected[6].

3. Unimodal Biometrics System

Biometric identification systems which use a single biometric trait of the individual for identification and verification are called unimodal systems.
When selecting a biometric trait for use in a particular application, the biometric trait is assessed on the following seven characteristics. These characteristics are different for each biometric type. These can be measured in High, Medium and Low[7] . A biometric modality should possess these seven characteristics in order to provide high performance and accuracy in biometric identification systems

1. **Universality:** Every person using a system should possess the trait.
2. **Uniqueness:** The trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
3. **Permanence:** The manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.
4. **Measurability:** The ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
5. **Performance:** The accuracy, speed, and robustness of technology used.
6. **Acceptability:** How well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.

Circumvention: The ease with which a trait might be imitated using an artifact or substitute

Biometric characteristics	Finger print	Hand geometry	Face	Iris	Voice
Universality	M	M	H	H	M
Uniqueness	H	M	H	H	L
Permanence	H	M	M	H	L
Performance	H	M	L	H	L
Measurability	M	H	H	M	M

Table 1: Comparison of biometric characteristics

3.1 Limitations of Unimodal System

Limitations of biometric systems using any single biometric characteristic:

1) **Susceptibility of the biometric sensor to noisy or bad data:** The captured biometric trait might be distorted due to imperfect acquisition conditions. This limitation can be seen in applications which use facial recognition. The quality of the captured facial images might get affected by illumination conditions and facial expressions. Another example could be in fingerprint recognition where a scanner is unable to read dirty fingerprints clearly and leads to false database matches. An enrolled user might be incorrectly rejected whereas an impostor might be falsely accepted.

2**) Intra-class variations:** Biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment. This variation is typically caused by a user who is incorrectly interacting with the sensor.

3) **Distinctiveness:** While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait. For example, Facial recognition may not work correctly for identical twins as the camera might not be able to distinguish between the two subjects leading to inaccurate matching.

4) **Non-universality:** While every user is expected to possess the biometric trait being acquired, in reality it is possible that a group of users do not posses that is possible that a group of users do not posses that particular biometric characteristic.

5) **Spoof attacks:** An individual may attempt to forge the biometric trait. This is particularly easy when signature and voice are used as an identifier. For example, fingerprint recognition systems can be easily spoofed using rubber fingerprints[8].

4. Multimodal Biometrics System

Limitations of unimodal biometric systems can be overcome by using multimodal biometric systems. Multimodal biometrics refers to the use of a combination of two or more biometric modalities in an identification system. For instance, a system that combines face and iris recognition can be considered as a multimodal biometric system. The most important reason behind using multimodal biometric systems is to improve the recognition rate [9].

4.1 Levels of integration

Information presented by multiple traits may be integrated at following levels:

a) Feature extraction level: At this level, the data obtained from each sensor is used to compute a feature vector. Since data from various traits are independent of each other they can be concatenated to a new vector with higher dimensionality that represents a person's identity in a new hyperspace. This new vector is then used in the matching and decision-making modules of the biometric system.

b) Matching score level: At this level, each individual system provides a matching score and those scores are combined to affirm the authenticity of the claimed identity.

c) Decision level: At this level, each individual system provides multiple biometric data and the resulting vectors are individually classified into two classes – accept or reject. Final decisions are consolidated by employing techniques such as majority voting.

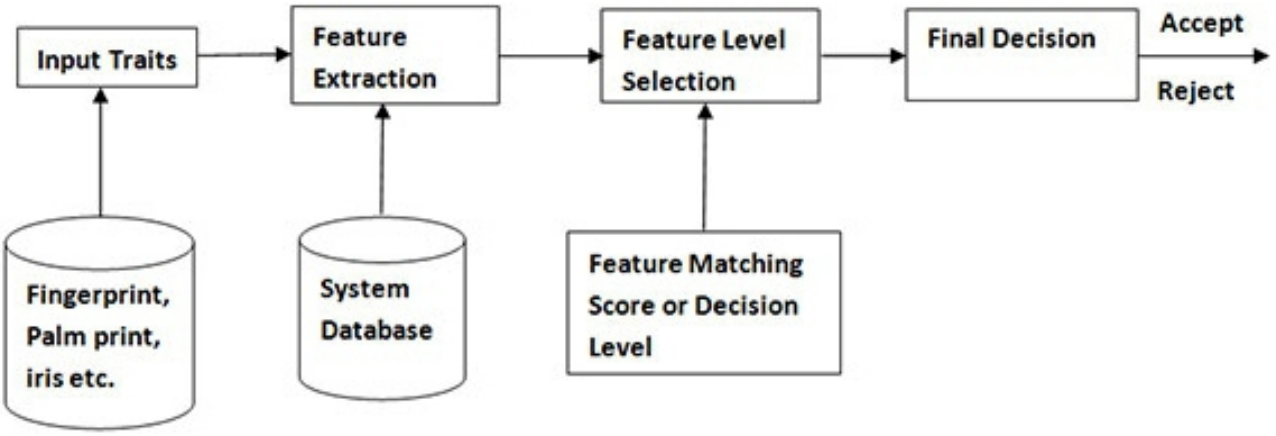

Figure 2: Block diagram of Multimodal Systems

Multimodal biometrics provides supplementary information among different modalities in order to increase the recognition performance in terms of accuracy and reliability to overcome the drawbacks of a single biometric system[10].

4.2 Advantages of multimodal biometrics system

1.Accuracy: The accuracy of a multimodal biometric system is measured by the errors in image acquisition and matching of the biometric traits. Image acquisition errors include failure-to-acquire (FTA) rate and failure-to-enroll (FTE) rate. Matching errors consist of false non-match rates (FNMR) in which a legitimate subject is rejected and a false match rate (FMR) where an intruder is granted access. Multimodal systems have almost zero FTA, FTE, FNMR and FMR rates.

2.Reduces data distortion: Multimodal biometrics can reduce data distortion. In cases where the quality of a biometric sample is unacceptable, the other biometric trait can be used. For example, if a fingerprint scanner rejects the fingerprint image due to poor quality using another biometric modality such as facial rejection will lower the false rejection rates.

3.Difficult to spoof: Multimodal biometric systems are very difficult to spoof as compared to unimodal systems. Even if one biometric modality could be spoofed, the individual can still be authenticated using the other biometric identifier[11].

5. Conclusion and Future Scope

Biometrics refers to an automatic recognition of a person based on his/her behavioral and/or physiological characteristics. In future, many business applications (e.g. banking) will rely on biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made.

Multimodal biometric system has the potential to be broadly applied in a wide range of civilian applications such as: banking security, check cashing and credit card transactions, information system security like access to databases via login privileges. Globally, the market for multimodal biometric systems is predicted to rise due to their increasing penetration in government and transportation application. The utilities of these systems in national IDs and biometric passports & visas majorly are boosting the multimodal biometric market. In future, an identity verification system based on the fusion of face and iris data can be designed as face recognition is friendly and non-invasive whereas iris recognition is one of the most accurate biometrics.

6. References

[1] Joseph Lewis, University of Maryland, Bowie State University, "Biometrics for secure Identity Verification: Trends and Developments",January 2002.

[2] Alsaadi IM (2015) Physiological biometric authentication systems, advantages disadvantages and future development: A review. Int J Sci Technol Res 12: 285-289.

[3] Kaur G, Singh G, Kumar V (2014) A review on biometric recognition. International Journal of Bio-Science and Bio-Technology 4: 69-76.

[4] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, March/April 2003, pp. 33-42.

[5] Kresimir Delac, Mislav Gregic, “A Survey of Biometric Recognition Methods”, 46th International Symposium Electronic in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia.
[6] A. H. Mir, S. Rubab and Z. A. Jhat, “Biometrics Verification: a Literature Survey", Journal of Computing and ICT Research, vol. 5, no. 2, pp. 67-80.

[7] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004.

[8] J. L. Wayman, “Fundamentals of Biometric Authentication Technologies", International Journal of Image and Graphics, Vol. 1, No. 1, pp. 93-113, 2001.

[9] A. K. Jain, A. Ross, "Multibiometric Systems", Appeared in Communication of the ACM, Special Issue on Multimodal Interfaces, Vol. 47, No.1, pp. 34-40, January 2004.
[10] L. Hong, A. K. Jain, S. Pankanti, "Can multibiometrics improve performance?" in Proc. AutoID'99, Summit, NJ, October 1999, pp. 59-64.

[11] Snelick, R., Indovina, M., Yen, J., and Mink, A. Multimodal biometrics: Issues in design and testing. In Proceedings of International Conference on Multimodal Interfaces (Vancouver, B.C., Nov. 5–7, 2003).