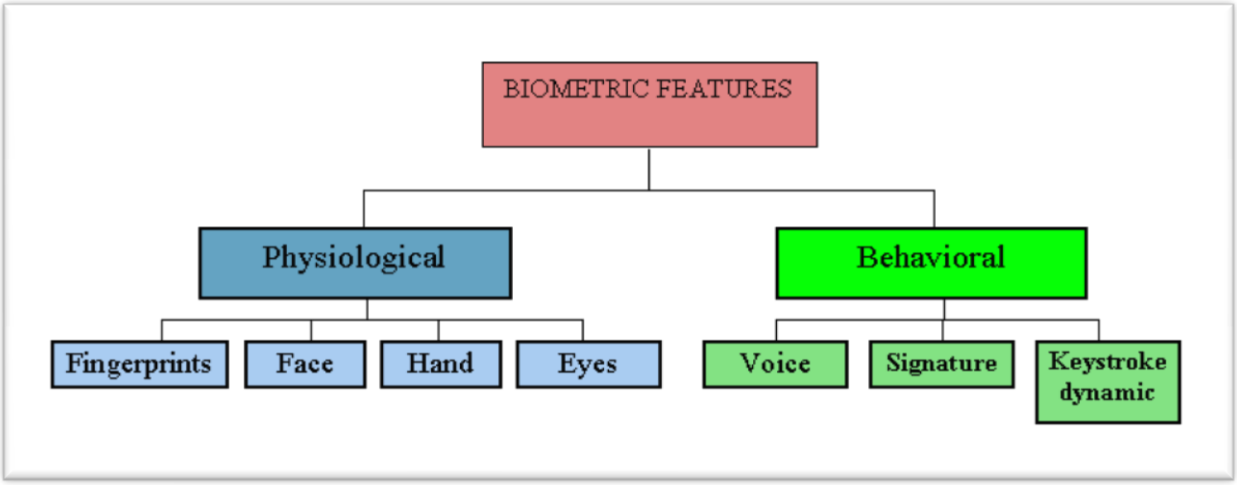
Biometrics: A Boon to Administration

Dr. D.V. Honagannavar
Principal, KLE's J.G.College of Commerce, Vidyanagar, Hubli.

Abstract: Biometrics technology measures and statistically analyses people's unique physical and behavioral characteristics. It is used for identification and access control of the individuals under surveillance. The basic principle of biometrics is 'authentication' it accurately identifies individuals by their intrinsic physical or behavioral traits. Authentication, by biometric verification is an advanced monitoring and security system in public security systems, administration and other techie applications. Adding to security, it's a driving force behind user verification and very convenient, as it does not require passwords or security tokens to be memorized. It's a bio friendly system with contactless operations.

Keywords: FRR (False Rejection Rate), FAR (False Acceptance Rate), Identity and Access Management (IAM).

Introduction: The Biometric Systems are automatic and technological methods thus used for verifying and recognizing the identity of a living person based on the physiological characteristics of that person, such as fingerprint, facial pattern and behavioral specifics. A biometric system which is based on physiological characteristics of a living person is more reliable in comparison with the one which adopts a living person behavioral feature, even if the behavioral feature may be easier to integrate within certain specific applications.



Whenever a transaction is made biometric characteristics is the only way which guarantees the presence of the owner. Specifically, fingerprint-based biometric systems have been effective in protecting the information and the resources in a large area of applications. At present scenario of pandemic these systems have played a major role in the administration with their unique feature of face, eyes impression. Before using these systems for verification or identification the users must be enrolled. The enrollment process involves the individual giving a sample of his or her biometric characteristic which is used by the system to generate a compact model which summarizes the distinctive features. On the basis of the application specificity these models can be databased/warehoused into a centralized database which can be distributed over a network, or can be stored in badges and rendered to the users. Each time an individual requires a verification or identification he or she provides a new sample of his or her fingerprint and the system matches this current instance with the stored model.

System Performance:

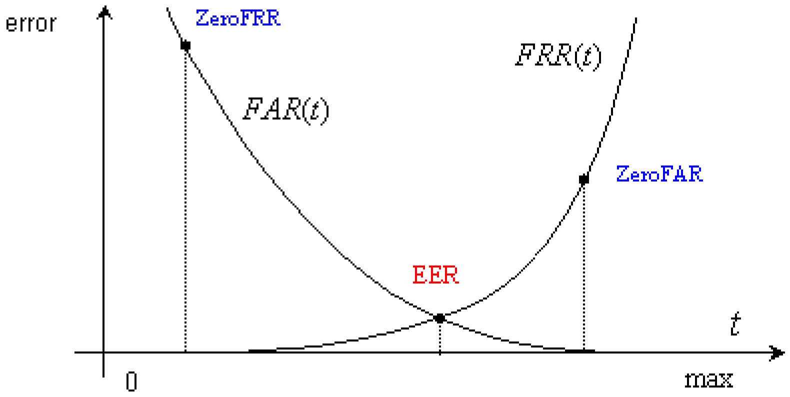
Based on the positioning on the biometric system sensor to environmental changes, from deformations to noise, it terms impossible that the two samples of the same biometric characteristic will be acquired in different sessions which exactly coincide and for this reason the matching is performed by an algorithm which computes a similarity score and compares it with an acceptance threshold, in which if the similarity is greater than the threshold, the system claims that the two samples coincide.

The main system's errors are usually calculated in terms of the following:

- FRR (False Rejection Rate) the frequency of rejections relative to people who should be accurately verified. When an authorized user is rejected then he or she must represent his or her biometric characteristic to the system. Any false rejection done by the system does not mean there exists an error in the system, rather, it might be a wrong positioning of the assigned finger on the sensor or dirt which can/may produce false rejections.

- FAR (False Acceptance Rate) is the frequency/magnitude of an unauthorized accesses, the reason being, impostors who claim a false identity.

Practically FAR and FRR depend on the acceptance threshold **'t'**, which is used to set the desired security level, being strictly related to each other. Specifically the FRR(t) is an increasing function and FAR(t) is a decreasing function hence, if the threshold setting is increased to make the access harder for impostors, certain authorized people may find it difficult/hassled to gain access.



The False acceptance rate (FAR) and the false rejection rate (FRR) are the functionalities against the threshold i.e. "t"

Identity and Access Management (IAM) plays a vital role in securing enterprise systems. It's is a framework for administrating digital identities and assigning individual user access to the resources. It provides the organizations with tools to regulate their access to systems or their data and reduce the risk of unauthorized access to secure resources or data soar/theft. It enables the organizations to quickly identify the data and where it is stored & accessed by whom.

It performs three key functions:

- Identification: through user-specific digital profiles containing unique identification information.
- Authentication: via username and password combinations, PIN numbers, one-time codes, etc.
- Authorization: by granting users access based on their role, access level, or other requirements.

As all the above functions are vital, the Authentication function is highly important as the organizational data is exposed to sensitive resources and other external users. Stronger authentication measures validate digital identities and lower the risk of unverified users trying to gain access to the organizational data. A successful IAM implementation requires a strong authentication and this can be achieved by incorporating behavioral biometrics which allows the organizations to offer a more positive authentication experience for their customers with greater security than the traditional forms of authentication. As more number of organizations implement strong authentication measures as part of their digital transformation, behavioral biometrics and advancing biometric security will continue playing a greater key role in demonstrating the impact of boosting authentication with biometrics to intruders from tampering the organizational data.

Conclusion:

The Biometric systems with the IMA systems thereby incorporate a complex, definitional, technological, and operational choices which thus are embedded in larger technological and social contexts with the system's-level considerations being critical factor. The thorough study analysis of a biometric system's performance, effectiveness, trustworthiness, and suitability should take a broader systems perspective. They should be designed and evaluated in relation to their specific intended purposes and contexts, rather than general/common purposes. Their effectiveness depends much on the social context as it does on the underlying technology, operating environment, systems engineering, and system testing regimes. The biometrics technology benefits in a rigorous and comprehensive manner when approached to systems for their development based on the organizational objectives, evaluation, and interpretation. Therefore Biometric systems are not a general replacement for other authentication technologies however combining biometric approaches with other security methods can augment those applications where user co-operation is a mandate.

Reference:

- Watson: Biometrics: Easy to Steal, and Hard to Regain Identity, Nature, vol. 449, 2007, p. 535
- The Consideration of Data Security in a Computer Environment, tech report G520-2169, IBM, 1970.
- D. Raphael, and J. Young, Automated Personal Identification, SRI, 1974.