BIOMETRICS- A REVIEW

Swati Sharma(Research Scholar) , Dr.S. S. Mehta(Prof)
Devendra Nagal(Research Scholar)
Department of Electrical Engineering
Jai Narain Vyas University
MBM Engineering College
Jodhpur-342001 , Rajasthan, India
er.swati.sharma15@gmail.com ,
ssmehta_58@rediffmail.com, devendra.nagal@gmail.com

Harleen Mehta
Christ University, Bangalore, India
mehta.harleen@gmail.com

Guneet Singh Mehta
Indian Institute of Technology, Jodhpur
mehta_guneet@iitj.ac.in

***Abstract*— An overview of biometrics has been presented in this paper. Biometrics deals with the study of fingerprint, face, iris, voice, signature and hand geometry. Many other modalities are in various stages of development and assessment. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. The two categories of biometric identifiers include physiological and behavioral characteristics. A biometrics would identify by using voice, DNA, hand print or behavior. Behavioral characteristics are related to the behavior of a person, including but not limited to: typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.**

Keywords- Biometrics, applications, modes of operation

I. INTRODUCTION

Biometrics has been around since 29,000 BC when cavemen would sign their drawings with handprints. In 500 BC Babylonian business transactions were signed in clay tablets with fingerprints. The earliest cataloging of fingerprints dates back to 1881 when Juan Vucetich started a collection of fingerprints of criminals in Argentina . Biometrics (ancient Greek: bios ="life", metron ="measure") is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In information technology, "biometric authentication" refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes. Examples of physical (or physiological or biometric) characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioral characteristics include signature, gait and typing patterns.

Any human physiological or behavioral characteristic could be a biometrics provided it has the following desirable properties : (*i*) *universality*, which means that every person should have the characteristic, (*ii*) *uniqueness*, which indicates that no two persons should be the same in terms of the characteristic, (*iii*) *permanence*, which means that the characteristic should be invariant with time and (*iv*) *collectability*, which indicates that the characteristic can be measured quantitatively.

In practice, there are some other important requirements : (*i*) *performance*, which refers to the achievable identification accuracy, the resource requirements to achieve an acceptable identification accuracy and the working or environmental factors that affect the identification accuracy, (*ii*) *acceptability*, which indicates to what extent people are willing to accept the biometric system, and (*iii*) *circumvention*, which refers to how easy it is to fool the system by fraudulent techniques.

Biometric techniques are providing a highly-secured identification and personal verification solutions thereby providing a robust solution to many challenging problems in security. The collection of Biometric characteristics is done using a device called a sensor used to acquire the data needed for verification or identification and to convert the data to a digital code. The quality of the device chosen to capture data has a significant impact on the recognition results. Among various devices, digital cameras can be used for face recognition, ear recognition etc or a telephone for voice recognition etc. A biometric system operates in verification mode or identification mode. In verification mode the system validation of a person identity is performed by comparing the captured biometric data with the biometric template stored in the database and is mainly used for positive recognition. In the identification mode the system captures the biometric data of an individual and searches the biometric template of all users in the database till a match is not found.

II. BIOMETRICS TECHNOLOGY

Adaptive biometric Systems aim to auto-update the templates or model to the intra-class variation of the operational data. The two-fold advantages of these systems are solving the problem of limited training data and tracking the temporal variations of the input data through adaptation. Recently, adaptive biometrics have received a significant attention from the research community. This research direction is expected to gain momentum because of their key promulgated advantages. First, with an adaptive

biometric system, one no longer needs to collect a large number of biometric samples during the enrollment process. Second, it is no longer necessary to re-enrol or retrain the system from the scratch in order to cope up with the changing environment. This convenience can significantly reduce the cost of maintaining a biometric system. Despite these advantages, there are several open issues involved with these systems. For mis-classification error (false acceptance) by the biometric system, cause adaptation using impostor sample. However, continuous research efforts are directed to resolve the open issues associated to the field of adaptive biometrics.

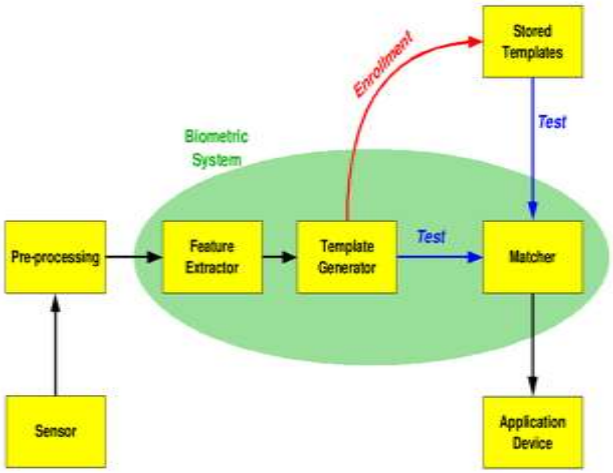

Fig. 1 The basic block diagram of a biometric system

No single biometrics is expected to effectively satisfy the needs of all identification (authentication) applications. A number of biometrics have been proposed, researched, and evaluated for identification (authentication) applications. Each biometrics has its strengths and limitations and accordingly, each biometric appeal to a particular identification (authentication) application. Some of the biometric technologies are:

a) Voice :

Voice is a characteristic of an individual. However, it is not expected to be sufficiently unique to permit identification of an individual from a large database of identities. Moreover, a voice signal available for authentication is typically degraded in quality by the microphone, communication channel and digitizer characteristics. Language independent speaker verification verifies a speaker identity irrespective of the language of the uttered phrase and is even more challenging.

b) Fingerprints:

Fingerprints are graphical flow-like ridges present on human fingers. Their formations depend on the initial conditions of the embryonic development and they are believed to be unique to each person (and each finger). Fingerprints are one of the most mature biometric technologies used in forensic divisions worldwide for criminal investigations and therefore, have a stigma of criminality associated with them. Typically, a fingerprint image is captured in one of two ways: (i) scanning an inked impression of a finger or (ii) using a live-scan fingerprint scanner.

Fig.2. Fingerprint

c) Face:

Face is one of the most acceptable biometrics because it is one of the most common methods of identification which humans use in their visual interactions Facial disguise is of concern in unattended authentication applications. It is very challenging to develop face recognition techniques which can tolerate the effects of aging, facial expressions, slight variations in the imaging environment and variations in the pose of face with respect to camera.

Fig.3. Fingerprint with labelling

d) Iris :

Visual texture of the human iris is determined by the chaotic morphogenetic processes during embryonic development and is posited to be unique for each person and each eye. An iris image is typically captured using a non-contact imaging process. Capturing an iris image involves cooperation from the user, both to register the image of iris in the central imaging area and to ensure that the iris is at a predetermined distance from the focal plane of the camera.

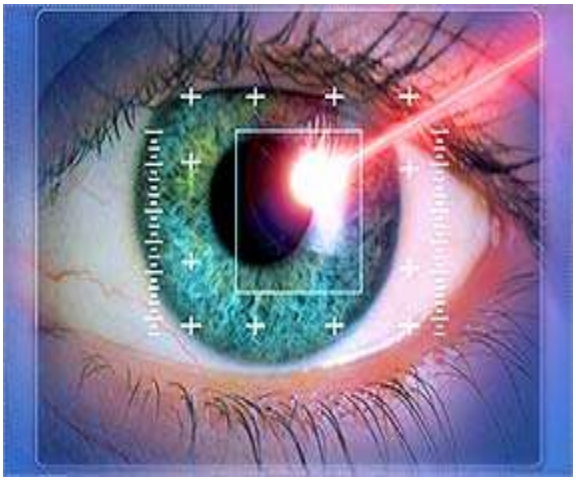

Fig.3. Identification based on Iris

e) Ear:

It is known that the shape of the ear and the structure of the cartilegenous tissue of the pinna are distinctive3. The features of an ear are not expected to be unique to each individual. The ear recognition approaches are based on matching vectors of distances of salient points on the pinna from a landmark location on the ear. No commercial systems are available yet and authentication of individual identity based on ear recognition is still a research topic.

III. MODES OF OPERATION

A biometric system can operate in the following two mode namely verification mode and identification mode. In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps involved in person verification.. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of verification mode, "where the aim is to prevent multiple people from using same identity".

In Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

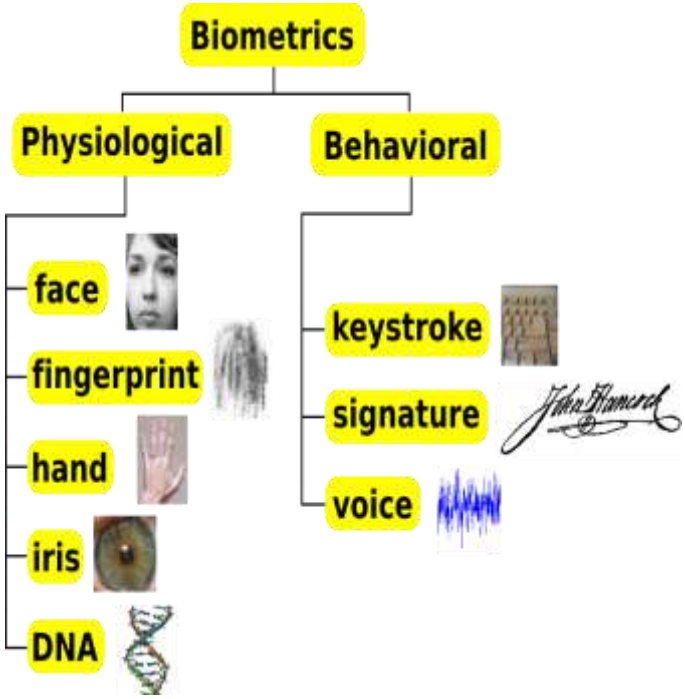

Fig.5. Approaches of biometrics

IV. ISSUES AND CONCERNS WITH CHALLENGING AREAS

One of the issue is privacy and discrimination in it which *is* possible that data obtained during biometric enrollment may be used in ways for which the enrolled individual has not consented. Another is danger to owners of secured items in which when thieves cannot get access to secure properties,

there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. Next issue is of cancelable biometrics which has advantage of passwords over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. Cancelable biometrics is a way in which to incorporate protection and the replacement features into biometrics incorporate protection and the replacement features into biometrics. Another is Soft biometrics which traits are physical, behavioral or adhered human characteristics, which have been derived from the way human beings normally distinguish their peers (e.g. height, gender, hair color). Those attributes have a low discriminating power, thus not capable of identification performance; additionally they are fully available to everyone which makes them privacy-safe.

Designing biometric sensors, which automatically recognize the operating environment (outdoor / indoor / lighting etc) and communicate with other system components to automatically adjust settings to deliver optimal data, is also the challenging area. The sensor should be fast in collecting quality images from a distance and should have low cost with no failures. Fundamental understanding of biometric technologies, operational requirements and privacy principles to enable beneficial public debate on where and how biometrics systems should be used, embed privacy functionality into every layer of architecture, protective solutions that meet operational needs, enhance public confidence in biometric technology and safeguard personal information.

V. Novel Applications

As biometric technology matures, there will be an increasing interaction among the (biometric) market, (biometric) technology and the (identification) applications. The emerging interaction is expected to be influenced by the added value of the technology, the sensitivities of the population, and the credibility of the service provider. It is too early to predict where and which biometric technology would evolve and be mated with which applications. Applications like automating identification for more convenient travel, for transactions via e-commerce, etc. seem to be ready for commercialization, but perhaps, biometric technology could open up a whole new genre of futuristic hi-tech applications that were not foreseen before. Following are some applications of biometrics :

- Biometric Time Clocks or Biometric time and attendance systems, which are being increasingly used in various organisations to control employee timekeeping.
- Biometric access control systems, providing strong security at entrances.
- Biometric systems are also developed for securing access to pc's and providing single logon facilities.
- Wireless biometrics for high end security and providing safer transactions from wireless devices like PDA's, etc.
- Applications of biometrics technology in identifying DNA patterns for identifying criminals, etc.
- Biometrics airport security devices are also deployed at some of the world's famous airports to enhance the security standards.

VI. Conclusion

In today's technology advancement era, where computers are a necessary nutrient to comply with and serve all the activities, the need for secured, reliable, simple and flexible system has advertently become a challenging concern for the organizations. The technology advancement has been a boon for speedy achievements of activity goals but at the same time the security breaches and transaction frauds are on rise. Thus, the Biometric Technology has taken its pace to prevent any security breaches and fraudulent. This technique measures unique physiological and behavioral features of individuals to identify and verify them as the right person for the crucial information. The physiological features include face, fingerprints, hand geometry, iris, retinal, DNA etc. and behavioral features include signature, study of keystroke, voice etc.Many countries like Australia, Brazl, Canada, Gambia , Germany, Israel, Iraq *a*nd India also applying biometrics. Interesting scenarios might materialize as a number of civilian applications of identification are integrated based on a single or multiple biometric technologies. This will certainly have a profound influence on the way we conduct our business. Biometrics is a science of automatically identifying individuals based on their unique physiological or behavioral characteristics. A number of civilian and commercial applications of biometrics-based identification are emerging. At the same time, a number of legitimate concerns are being raised against the use of biometrics for various applications; three of them appear to be the most significant: cost, privacy and performance. For the wide-spread use of the biometrics to materialize, it is necessary to undertake systematic studies of the fundamental research issues underlying the design and evaluation of identification systems. Further, it is critical to engineer the match between the application needs and the available technologies.

REFERENCES

[1] A. Rattani, B. Freni, G. L. Marcialis and F. Roli,"*Template update methods in adaptive biometric systems: a critical review*," 3rd International Conference on Biometrics, Alghero, Italy, pp. 847-856, 2009 .

[2] Jain, A., Hong, L., & Pankanti, S. (2000). "Biometric Identification". Communications of the ACM, 43(2), p. 91-98.

[3] Magnuson, S . "Defense department under pressure to share biometric data." NationalDefenseMagazine.org. Retrieved 20 February 2010.

[4] Mane Vijay M and Jadhav Dattatray V "Review of Multimodal Biometrics: Applications, challenges and Research Areas", International Journal of Biometrics and Bioinformatics (IJBB), Volume 3, Issue 5

[5] Sahoo, SoyujKumar; Mahadeva Prasanna, SR, Choubisa, Tarun "Multimodal Biometric Person Authentication : A Review", *IETE Technical Review*,2012

[6] Weaver, A.C. "Biometric Authentication". *Computer*, 39 (2), p. 96-97,2006.