

## DNA Biometric

Suvarnsing G. Bhable<sup>1</sup>, Sangramsing Kayte<sup>1</sup>, Raju Maher<sup>2</sup>, Jaypalsing Kayte<sup>3</sup>,  
<sup>4</sup>Dr. Charansing Kayte

<sup>1, 2, 3</sup>(Department of CS & IT, Dr.B.A.M.University, Aurangabad, India)

<sup>4</sup>Department of Digital and Cyber Forensic Aurangabad, Maharashtra, India.

---

**Abstract :** *The biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Biometrics has been in the development for many years and with the recent advancements in technology has made some biometrics affordable and more reliable. Our goal is to show how DNA biometrics can improve the network security scheme of an organization. The process of biometrics will be broken down by its process and limitations, accessibility, accuracy, and use with applications. That's why DNA Biometric is essential to make for best recognition.*

**Keywords -** Biometric, DNA,

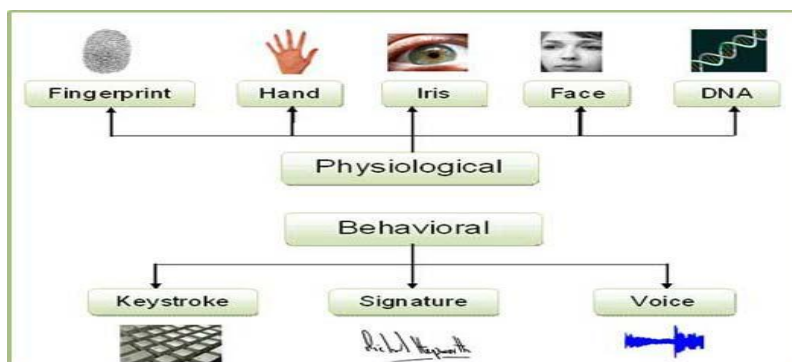
---

### I. Introduction

“Biometrics” is a term used in many aspects of our world. It is no longer a term known only to the government or “secret research organizations”. Biometrics is characterized by physical features of a being and measurement of those features. When the general public hears biometrics, the first thought that may come to mind would probably be “fingerprints”. Fingerprint biometrics is the most established and used form of identification and verification today and has been since as early as 500 B.C. However, there are other biometric systems that began to emerge in the latter half of the twentieth century, coinciding with the introduction of computer systems. Most commonly studied or implemented biometrics is: fingerprint, face, iris, voice, signature and hand geometry. There is not just one model that is best for all situations. There are many factors that must be taken into account in planning stages, such as: Location, security risks, task, number of users, user circumstances, existing data etc. Biometrics is being used by many organizations as added security to already established measures. Determining the most effective biometric technology is based on how and where it will be used. Each modality has its strengths and weaknesses. Those requirements should be determined during the planning stages prior to implementation. There are other modalities in various stages of development and assessment today, DNA being one of them. Of all the biometric identification systems, DNA provides the most reliable form of identification. DNA is intrinsically digital and unchangeable during a human's life and even after death. So, why is it so complex for DNA to be used today? There are many complexities surrounding the issue of Biometrics of DNA, such as: Biometrics and health issues, private information, invasion of civil liberties, access to DNA and data, uncompromised storage of DNA and extraction and process time.

### II. Biometrics

Biometric characteristics can be divided into two main categories: psychological and behavioral. Physiological are based on the shape of the body. Fingerprints are one of the physiological traits that have been used for more than 100 years. Other physiological traits are face recognition, hand geometry and iris recognition. Behavioral characteristics are related to the behavior of a person. The signature is a widely used form of identification and verification. Other behavior approaches are voice recognition and keystroke behavior. Other biometrics being researched and developed are based on a persons' way of walking, also known as their “gait”, retina, hand veins, ear recognition, facial thermo gram, DNA, odor and palm prints.



"Fig.1 Biometrics Classification"

### III. Biometric Comparison

Human characteristics are easier understood using the following parameters;

- a. Uniqueness – How well the biometric separates individually from another.
- b. Performance – How well a biometric resists aging
- c. Collectability – Ease of acquisition for measurement.
- d. Performance – Accuracy, speed, and robustness of technology used.
- e. Acceptability – Degree of approval of a technology.
- f. Circumvention – Ease of use of a substitute.

A biometric system can perform two functions: verification and identification. Verification of an individual uses a direct sample and compares that sample to a pre-stored template. Identification is done by comparing the direct sample to the pre-stored template and finding the best batch. The DNA row on the above table illustrates a high ranking in the categories which are vital to certainly identifying an individual with minimal false acceptance rate (FAR). The columns with the low ranking, with exception to the collectivity column, are in direct correlation with current legal issues pertaining to security of person information, secure storage, accessibility and invasion of privacy. These issues will be covered in further detail in the DNA Social Concerns section of this report.

### IV. DNA Is Biometrics

First of all, DNA differs from standard biometrics in several ways:

- a. DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples
- b. DNA requires a tangible physical sample as opposed to an impression, image, or recording.
- c. DNA matching is not done in real-time, and currently not all stages of comparison are automated.

Regardless of these basic differences, DNA is a type of biometric inasmuch as it is the use of a physiological characteristic to verify or determine identity. DNA testing is a technology with a high degree of accuracy (as shown in the table on pg 1); however, the possibility of sampling contamination and degradation will pose an impact on the accuracy of the method.

### V. Dna Sociological Concerns

#### A. Invasion of Civil Liberties

The use of biometric technology raises concerns for individuals. DNA is a highly informative piece of information that some feel can be used for negative means if given the opportunity. With this in mind, the nature of DNA and its use in the biometric environment can be threatening and an invasion of the fourth amendment of the constitution – Guards against seizure of property specifically in a non-criminal environment.

#### B. Storage of DNA

There are two main security problems for the securing of a DNA system (access rights, use of information only for the overriding purpose), and the implementation of security mechanisms in order to ensure for instance a high level of confidentiality and the security of DNA database (access rights, length of information retention). Currently, the National Science and Technology Council (NTSC), Committee on Technology, Committee on Homeland and National Security and Subcommittee on Biometrics are part of the

internal deliberative process of NTSC. These agencies develop and implement multi-agency policies that aid in moving the biometric sciences to meet public and private needs.

### **VI. Access To DNA**

One of the primary concerns by individuals and legal experts is the accessibility to private information. Unauthorized access and use of personal information by the government, insurance agencies, judicial systems and people and organizations for illegal gain is invasive and intimidating. There are three primary laws that apply to government held personal information: The Freedom of Information Act that usually provides access to any government record to anyone for any purpose. This act is subject to specific exceptions that includes protection of personal privacy. The Privacy Act of 1974 is a collection of principles that govern the governments use, collection and maintenance of personally identifiable information contained in a system of records. The E-Government Act of 2002 requires government agencies to access their use of information technology and its impact on privacy.

### **VII. Health Issues**

Most of the biometric systems in place today use sensors to obtain the individual's biometric information. The majority of health concerns are those we encounter in our daily lives such as: touching a handprint sensor. This type of concern is in direct relation to touching a doorknob in a public place. However, there are other concerns specifically related to scanning devices. There are fears that the devices can create health issues when the iris is scanned or when the face is scanned.

### **VIII. Advances Of DNA Biometrics**

The analysis of DNA took weeks and even months to process. With steady and resilient research, developers have been able to reduce the entire process down to less than 30 minutes. Organizations such as NEC have developed the world's first portable human DNA analyzer. This unit integrates all steps of the DNA analysis process and is able to do so in approximately 25 minutes (Tech News). Although this is completely unsuitable for access to a secure facility and is unacceptable to use in a Security Network environment, advances are being made to expedite the analysis process. While biometric standards, privacy issues, financial expectations, accuracy and various other topics are in question, developers continue to work closely with the NSTC and other technological organizations to investigate and improve the DNA biometric process.

### **IX. Conclusion**

Biometrics is the great promise for private, public and governmental agencies. The reality is that biometrics is the future of the security industry and is quickly becoming recognized as the most accurate identification technology in the market. Developers of biometric technology continue to search for easier and cost-effective means to secure user implementation. Companies adding biometrics to enhance the security of e-business systems hope to add value to user verification while maintaining customer satisfaction and accuracy. Biometrics products are becoming more flexible, capable of serving different purposes, or being used in tandem, accomplishing more than authentication.

### **References**

- [1]. United States. National Science and Technology Council (NSTC). Biometrics Frequently Asked Questions September 7, 2006. <http://www.biometrics.gov/docs/faq.pdf>.
- [2]. Biometrics. Jain, A. K. April 28-30, 2004. <http://en.wikipedia.org/wiki/Biometrics>.
- [3]. Development of Biometric DNA Ink for Authentication Security. Hashiyada, Masaki, July, 2004. <http://www.sasappa.co.jp/online/abstract/tmp/1/204/html/0112040202.html>
- [4]. Portable DNA Analyzer. Tech News. October 16, 2007. Portable DNA Analyzer
- [5]. Sangramsing Kayte, Suvarnsing G.Bhable and Jaypalsing Kayte, —A Review Paper on Multimodal Biometrics System using Fingerprint and Signature. IJCA Volume 128 – No.15, October 2015.
- [6]. United States. National Institute of Standard and Technology. Privacy & Biometrics, Building a Conceptual Foundation Pg. 4-52. September 15, 2006. <http://www.biometrics.gov/docs/privacy.pdf>.