BIOMETRICS

The word “biometrics” came from Greek and we can divide it into two roots: “bio” means life and “metrics” – to measure.
Biometrics is the automated recognition of individuals based on their behavioral and biological characteristics. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known) and consequently that they belong to a group with certain rights (or to a group to be denied certain privileges). It relies on the presumption that individuals are physically and behaviorally distinctive in a number of ways.

Biometric systems are used increasingly to recognize individuals and regulate access to physical spaces, information, services, and to other rights or benefits, including the ability to cross international borders.
The motivations for using biometrics are diverse and often overlap. They include improving the convenience and efficiency of routine access transactions, reducing fraud, and enhancing public safety and national security.
Questions persist, however, about the effectiveness of biometric systems as security or surveillance mechanisms, their usability and manageability, appropriateness in widely varying contexts, social impacts, effects on privacy, and legal and policy implications.

Biometric recognition, or biometrics, refers to the automated recognition of individuals based on their biological and behavioral characteristics. Biometric technology makes a contribution to crime detection by associating the traces to the persons Stored in the database, ranking the identity of persons and selecting subdivision of persons from which the trace may originate

Biometrics covers a variety of technologies in which unique identifiable attributes of people are used for identification and authentication. These include (but are not limited to) a person’s fingerprint, iris print, hand, face, voice, gait or signature, which can be used to validate the identity of individuals seeking to control access to computers, airlines, databases and other areas which may need to be restricted.

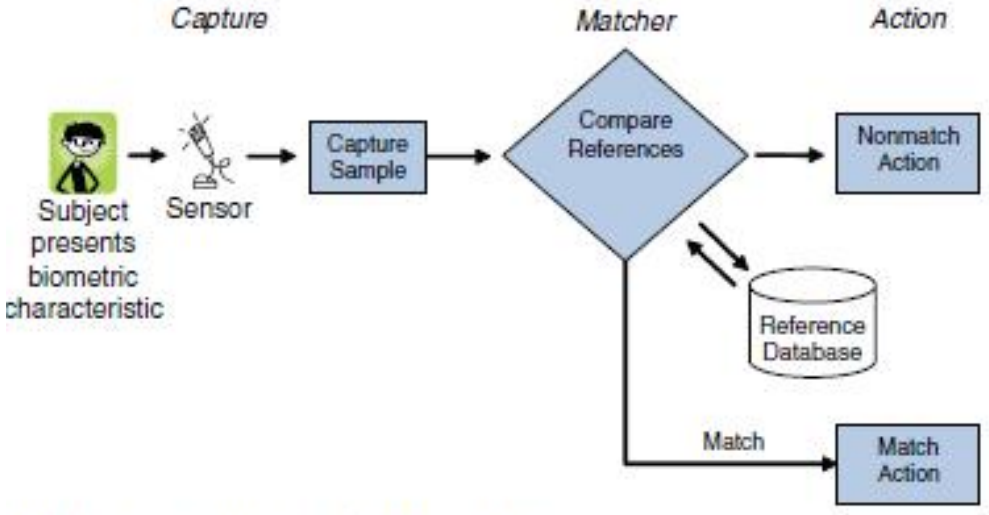


FIGURE 1.1 Operation of a biometric system.

The following are the principal conclusions:
• Human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated.
System designers and operators should anticipate and plan for the occurrence of errors, even if errors are expected to be infrequent.
• The scientific basis of biometrics—from understanding the distributions of biometric traits within given populations to how humans interact with biometric systems—needs strengthening

particularly as biometric technologies and systems are deployed in systems of national importance.

• Biometric systems incorporate complex definitional, technological, and operational choices, which are themselves embedded in larger technological and social contexts. Thus, systems-level considerations are critical to the success of biometric systems. Analyses of biometric systems' performance, effectiveness, trustworthiness, and suitability should take a broad systems perspective.

• Biometric systems should be designed and evaluated relative to their specific intended purposes and contexts rather than generically. Their effectiveness depends as much on the social context as it does on the
underlying technology, operational environment, systems engineering, and testing regimes.

• The field of biometrics would benefit from more rigorous and comprehensive approaches to systems development, evaluation, and interpretation. Presumptions and burdens of proof arising from biometric recognition should be based on solid, peer-reviewed studies of the performance of biometric recognition mechanisms.

Biometric characteristics of a person are unique. Most of such keys are impossible to copy and exactly produce. Theoretically these are ideal keys. But by using biometric identification a lot of specific problems appear.

All biometric identifiers can be divided into two big groups:

1) Physiological

2) Behavioral

CHEMICAL

DNA Matching

The identification of an individual using the analysis of segments from DNA.

VISUAL

Ear

The identification of an individual using the shape of the ear.

Eyes - Iris Recognition

The use of the features found in the iris to identify an individual.

Eyes - Retina Recognition

The use of patterns of veins in the back of the eye to accomplish recognition.

Face Recognition

The analysis of facial features or patterns for the authentication or recognition of an individuals identity. Most face recognition systems either use eigenfaces or local feature analysis.

Fingerprint Recognition

The use of the ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual.

VISUAL/SPATIAL

Finger Geometry Recognition

The use of 3D geometry of the finger to determine identity.

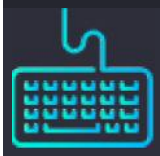
Hand Geometry Recognition

The use of the geometric features of the hand such as the lengths of fingers and the width of the hand to identify an individual.

BEHAVIOURAL

Gait

The use of an individuals walking style or gait to determine identity.



Typing Recognition

The use of the unique characteristics of a persons typing for establishing identity.

OLFACTORY

Odour

The use of an individuals odor to determine identity.

VEIN

Vein Recognition

Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger or palm.

AUDITORY

Voice - Speaker Identification

Identification is the task of determining an unknown speaker's identity. Speaker identification is a 1:N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc. For example, a police officer compares a sketch of an assailant against a database of previously documented criminals to find the closest match(es). In forensic applications, it is common to first perform a speaker identification process to create a list of "best matches" and then perform a series of verification processes to determine a conclusive match.

Voice - Speaker Verification/Authentication

The use of the voice as a method of determining the identity of a speaker for access control. If the speaker claims to be of a certain identity and the voice is used to verify this claim. Speaker verification is a 1:1 match where one speaker's voice is matched to one template (also called a "voice print" or "voice model"). Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking). These systems operate with the user's knowledge and typically require their cooperation. For example, presenting a person's passport at border control is a verification process - the agent compares the person's face to the picture in the document.

VISUAL/BEHAVIOURAL

Signature Recognition

The authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances algorithms. Dynamic is becoming more popular as ceremony data is captured along with the X,Y,T and P Coordinates of the signor from the signing device. This data can be utilized in a court of law using digital forensic examination tools, and to create a biometric template from which dynamic signatures can be authenticated either at time of signing or post signing, and as triggers in workflow processes.

Note: There is a difference between speaker recognition (recognizing who is speaking) and speech recognition (recognizing what is being said). These two terms are frequently confused, as is voice recognition. Voice recognition is a synonym for speaker, and thus not speech, recognition. In addition, there is a difference between the act of authentication (commonly referred to as speaker verification or speaker authentication) and identification.

FUNDAMENTALS OF BIOMETRIC RECOGNITION AND HUMAN INDIVIDUAL DISTINCTIVENESS

Biometric recognition systems are inherently probabilistic, and their performance needs to be assessed within the context of this fundamental and critical characteristic. Biometric recognition involves matching, within a tolerance of approximation, of observed biometric traits against previously collected data for a subject. Approximate matching is required due to the variations in biological attributes and behaviors both within and between persons. Consequently, in contrast to the largely binary results associated with most information technology systems, biometric systems provide probabilistic results.

There are numerous sources of uncertainty and variation in biometric systems, including the following:

• *Variation within persons.*

Biometric characteristics and the information captured by biometric systems may be affected by changes in age, environment, disease, stress, occupational factors, training and prompting, intentional alterations, sociocultural aspects of the situation in which the presentation occurs, changes in human interface with the system, and so on. As a result, each interaction of the individual with the system (at enrollment, identification, and so on) will be associated with different biometric information. Individuals attempting to thwart recognition for one reason or another also contribute to the inherent uncertainty in biometric systems.

• *Sensors.*

Sensor age and calibration, how well the interface at any given time mitigates extraneous factors, and the sensitivity of sensor performance to variation in the ambient environment (such as light levels) all can play a role.

• *Feature extraction and matching algorithms.*

Biometric characteristics cannot be directly compared but require stable and distinctive "features" to first be extracted from sensor outputs. Differences in feature extraction algorithms affect performance, with effects sometimes aggravated by requirements for achieving interoperability among proprietary systems.

Differences between matching algorithms and comparison scoring mechanisms, and how these interact with the preceding sources of variability of information acquired and features extracted, also contribute to variation in performance of different systems.

• *Data integrity.*

Information may be degraded through legitimate data manipulation or transformation or degraded and/or corrupted owing to security breaches, mismanagement, inappropriate compression, or some other means. It may also be inappropriately applied to a context other than the one for which it was originally created, owing to mission creep (for example, using the data collected in a domain purely for the sake of convenience in a domain that demands high data integrity) or inappropriate re-use of information (for instance, captured biometric information might be incorrectly assumed to be of greater fidelity when transferred to a system where higher fidelity is the norm).

Another fundamental characteristic of biometric recognition is that it requires decision making under uncertainty by both the automated recognition system and the human interpreters of its results. A biometric match represents not certain recognition but a probability of correct recognition, while a non match represents a probability rather than a definitive conclusion that an individual is not known to the system.

History of the Field—Two Biometrics

"Biometrics" has two meanings, both in wide use. The subject of this report—the automatic recognition of individuals based on biological and behavioral traits—is one meaning, which apparently dates from the early 1980s. In biology, agriculture, medicine, public health, demography, actuarial science, and fields related to these, "biometrics," "biometry," and "biostatistics" refer almost synonymously to statistical and mathematical methods for analyzing data in the biological sciences. This usage stems from the definition of biometry, proffered by the founder of the then-new journal *Biometrika* in its 1901 debut issue: "the application to biology of the modern methods of statistics." The writer was the British geneticist Francis Galton, who made important contributions to fingerprinting as a tool for identification of criminals, to face recognition, and to the central statistical concepts of regression analysis, correlation analysis, and goodness of fit.

Thus, the two meanings of "biometrics" overlap both in subject matter—human biological characteristics—and in historical lineage. Stigler (2000) notes that others had preceded the *Biometrika* founders in combining derivatives of the Greek βιος (bios) and μετρον (metron) to have specific meanings.[1] These earlier usages do not survive.

Johns Hopkins University opened its Department of Biometry and Vital Statistics (since renamed the Department of Biostatistics) in 1918. Graduate degree programs, divisions, and service courses with names incorporating "biostatistics," "biometrics," or "biometry" have proliferated in academic departments of health science since the 1950s. The American Statistical Association's 24 subject-matter sections began with the Biometrics Section in 1938, which in 1945 started the journal *Biometrics Bulletin*, renamed *Biometrics* in 1947. In 1950 *Biometrics* was transferred to the Biometric Society (now the International Biometric Society), founded in 1947 at Woods Hole, Massachusetts. The journal promotes "statistical and mathematical theory and methods in the biosciences through . . . application to new and ongoing subject-matter challenges." Concerned that *Biometrics* was overly associated with medicine and epidemiology, in 1996 the Society and the American Statistical Association jointly founded the *Journal of Agricultural, Biological, and Environmental Statistics* (*JABES*). The latter, along with other journals such as *Statistics in Medicine* and *Biostatistics*, have taken over the original mission of *Biometrika*, now more oriented to theoretical statistics.

Automated human recognition began with semiautomated speaker recognition systems in the 1940s. Semiautomated and fully automated fingerprint, handwriting, and facial recognition systems emerged in the 1960s as digital computers became more widespread and capable. Fully automated systems based on hand geometry

and fingerprinting were first deployed commercially in the 1970s, almost immediately leading to concerns over spoofing and privacy. Larger pilot projects for banking and government applications became popular in the 1980s. By the 1990s, the fully automated systems for both government and commercial applications used many different technologies, including iris and face recognition.

Clearly both meanings of biometrics are well-established and appropriate and will persist for some time. However, in distinguishing our topic from biometrics in its biostatistical sense, one must note the curiosity that two fields so linked in Galton's work should a century later have few points of contact. Galton wished to reveal the human manifestations of his cousin Charles Darwin's theories by classifying and quantifying personal characteristics. He collected 8,000 fingerprint sets, published three books on fingerprinting in four years,[2] and proposed the Galton fingerprint classification system extended in India by Azizul Haque for Edward Henry, Inspector General of Police, in Bengal. It was documented in Henry's book *Classification and Uses of Finger Prints*. Scotland Yard adopted this classification scheme in 1901 and still uses it.

But not all of Galton's legacy is positive. He believed that physical appearances could indicate criminal propensity and coined the term "eugenics," which was later used to horrific ends by the Third Reich. Many note that governments have not always used biologically derived data on humans for positive ends.

Galton's work was for understanding biological data. And yet biostatisticians, who have addressed many challenges in the fast-moving biosciences, have been little involved in biometric recognition research. And while very sophisticated statistical methods are used for the signal analysis and pattern recognition aspects of biometric technology, the systems and population sampling issues that affect performance in practice may not be fully appreciated. That fields once related are now separate may reflect that biometric recognition is scientifically less basic than other areas of interest, or that funding for open research is lacking, or even that most universities have no ongoing research in biometric recognition. A historical separation between scientifically based empirical methods developed specifically in a forensic context and similar methods more widely vetted in the open scientific community has been noted in other contexts and may also play a role here.[3,4]

Standards and Protocols

A lot of work has been done on the development of biometric standards.

International Standards

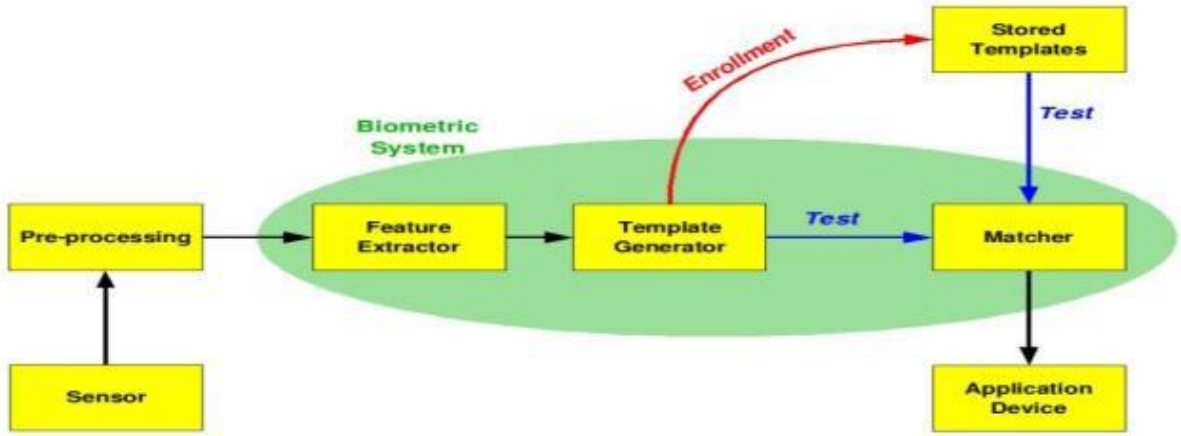
ISO (the International Organization for Standardization) and IEC (the International Electro technical Commission) form the specialized system for worldwide standardization. National Bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity.

In the field of information technology, ISO and IEC have established a Joint Technical Committee 1: ISO/IEC JTC 1 on Information Technology.

1. HTTP://WWW.ISO.ORG/ISO/STANDARDS_DEVELOPMENT/TECHNICAL_COMMITTEES/LIST_OF_ISO_TECHNICAL_COMMITTEES/ISO_TECHNICAL_COMMITTEE.HTM?COMMID=313770

2. HTTPS://WWW.ISO.ORG/COMMITTEE/45144.HTML

Biometric traits are inherent to individual and they are unique. Even two same resembling twins have different biometric traits.
Biometric system works in four stages.
(i)Enrollment Unit: This unit is also called sensor module. It acquires the raw biometric data of an individual in the form of an image, video, audio or some other signal.
(ii) Feature Extraction Unit: The feature extraction module operates on the biometric signal and extracts a salient set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user‘s identity, is stored in the biometric system and is known as a template.
(iii) Matching Unit: This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user‘s master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one too many matching).
(iv)Decision Maker: This module accepts or rejects the user based on a security threshold and matching score.Figure below shows the basic structure of biometric authentication system.



BIOMETRICS AND FORENSICS

Biometrics has been used for a long time in forensic science. Forensic science at crime scene is deeply influenced by Locard's exchange principle that states that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.

In his book Crime Investigation: Physical Evidence and the Police Laboratory, Kirk articulates the principle as follows : “Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibbers’ from his clothes, the glass he breaks, the tool marks he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value.”

From a long back face, hand writing, threads from the cloth, hairs have been used as the evidence by the forensic Science for the identification of the criminal or the missing person. In year 1892 the first textbook on the biometrics and forensic science was authored by Sir Francis.

System of personal identification by bodily measurements developed by French policeman Bertillon became famous. It was known as Bertillon system.

BIOMETRIC TRAITS USE IN FORENSIC SCIENCE:

Biometric traits are unique to individual and even to similar looking person or twins can‘t have same biometric traits. So they are very helpful at the time of criminal investigation. Here we will discuss about various biometric traits use in forensic science.

a) **FINGERPRINT**
b) FACE BIOMETRICS
c) DNA BIOMETRICS
d) PALMPRINT BIOMETRICS
e) IRIS BIOMETRICS
f) VOICE BIOMETRICS

Principle:

Users and developers of biometric systems should recognize and take into account the limitations and constraints of biometric systems especially the probabilistic nature of the underlying science, the current limits of knowledge regarding human individual distinctiveness, and the numerous sources of uncertainty in biometric systems.

Relevant CASES:

In order to find out whether Biometrics and forensic science are linked with each other from a long time or not let‘s look at few famous cases cracked using biometrics**.**

(i) **Ted Bundy(**evidence in this case were bite marks of criminal and fibers of victims cloth**)** Ted Bundy was serial killer responsible for an estimated 30-plus murder, when he was arrested in 1975; there were little physical evidences which prove his crime. Two years later, having been convicted only of kidnapping, Bundy was preparing to stand trial for murder in Colorado when he escaped and headed to Florida. There, he killed three more people early in 1978, and when he was finally captured in February of that year, the physical evidence in those cases led to his conviction. Most crucial was the matching of a bite mark on the buttock of victim Lisa Levy to the Bundy‘s distinctive, crooked and chipped teeth. He was convicted also of the murder of 12-year-old Kimberly Leach based on fibers found in his van that matched the girl‘s clothing. Bundy was put to death in 1989.

(ii) **(ii) The Lindbergh Kidnapping** (Biometric evidence in this case was handwriting of kidnapper) On March 1, 1932, Charles Lindbergh Jr., the 20-month-old son of the famous aviator, was kidnapped, and although a ransom of $50,000 was paid, the child was never returned. Tracking the circulation of the bills used in the ransom payment, authorities were led to Bruno Hauptmann, who was found with over $14,000 of the money in his garage. While Hauptmann claimed that the money belonged to a friend, key testimony from handwriting analysts matched his writing to that on the ransom notes. Additional forensic research connected the wood in Hauptmann‘s attic to the wood used in the make-shift ladder that the kidnappers built to reach the child‘s bedroom window. Hauptmann was convicted and executed in 1936.

(iii) **The Green River Killer (**Biometric data used in this case was the DNA sample) The Green River Killer was responsible for a rash of murders — at least 48 but possibly close to 90 — along the Green River in Washington state in the ‘80s and ‘90s. Most of the killings occurred in 1982-83, and the victims were almost all prostitutes. One of the suspects that police had identified as early as 1983 was Gary Ridgway, a man with a history of frequenting and abusing prostitutes. However, although they collected DNA samples from Ridgway in 1987, the technology available didn‘t allow them to connect him to the killings. It wasn‘t until 2001 that new DNA techniques spurred the

reexamination of evidence that incriminated Ridgway. He was arrested and later confessed. Ridgway pleaded guilty to 48 murders — later confessing to even more, which remain unconfirmed — in exchange for being spared the death penalty. He was sentenced to 48 life sentences without the possibility of parole.

There are so many of cases from early 80‘s till present where biometric used with forensic science and help in the true or correct identification of the wrongdoer. With the advancement in technology day by day criminals are using new tricks for conducting the crime. Therefore, accurate and efficient identification have become a vital requirement for forensic application due to diversities of criminal activities. A recent advancement in biometric technology which is equipped with computational intelligence techniques is replacing manual identification approaches in forensic science.