Chapter 1

Introduction

1.1 Historical Background

Biometrics is the study of anatomical and behavioral features of living beings, for the purpose of their automatic identification. This field of study was first introduced by Alphonse Bertillon (a French policeman) in the late nineteenth century. He developed the Bertillonage system, which was originally a set of tools used for identifying criminals. He primarily measured an array of certain anatomical traits of a person, including head length, head breadth, the length of the middle finger, the length of the left foot, and the length of the forearm [1]. A schematic diagram of these measurements is shown in Figure 1.1. These measurements were taken from suspected convicts and subsequently compared with the existing records (of former convicts) for a possible match.

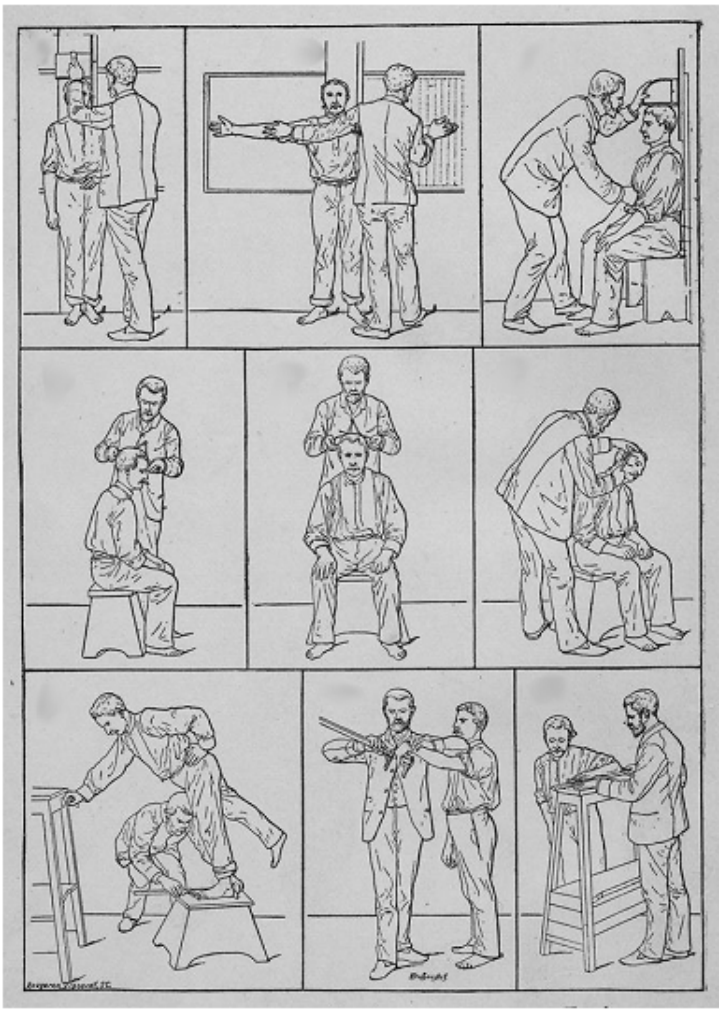

FIGURE 1.1: Various measurements taken under the Bertillonage system. From left to right and then top to bottom the figures show measurement of height, reach, trunk, length of head, width of head, right ear, left foot, left middle finger, and left forearm

The Bertillonage system, however, lacked in many aspects; the most significant ones being error intolerant, cumbersome to administer and inability to handle intra-class variations. Consequently, it was abandoned and replaced with a more accurate approach involving manual comparison of human fingerprints. The pioneering works of Henry Faulds [2], William Herschel [3], and Sir Francis Galton [4] facilitated in such endeavors, wherein the uniqueness of certain features in a fingerprint ridge

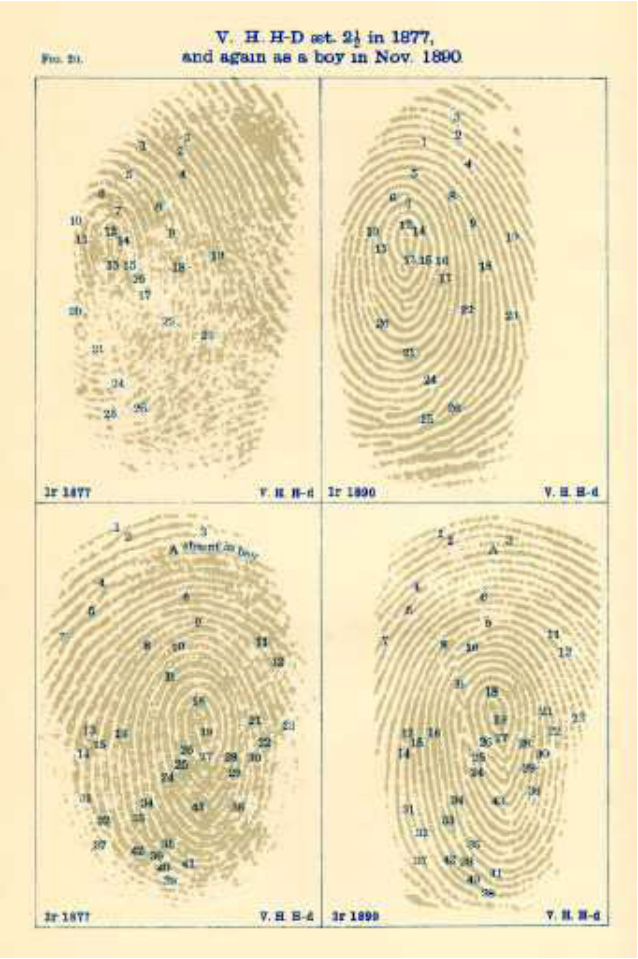

FIGURE 1.2: Variation of a child's fingerprints over time

pattern was established [5]. Specially Galton made some remarkable observations involving fingerprints which included providing a proof of the fact that a child's fingerprint remains same over time (illustrated in Figure 1.2).

With the continuous development of technology, the matching procedure of fingerprints gradually changed from manual to automatic [6]. Apart from fingerprints, researches in the utilization of other biometric traits were also conducted alongside. For instance, biometric systems based on face [7], iris [8] and palmprints [9] were successfully studied and subsequently patented. As implicitly presented in later

chapters, each biometric trait is unique in its own way and has some inherently associated pros and cons with them.

Biometric system frameworks have successfully replaced traditional token based access granting mechanisms like passwords and PIN numbers. The overwhelming success of biometric system can be attributed to the low level of security offered by the token based systems. For instance, passwords can be forgotten or guessed while tokens can be lost or stolen. Alternatively, biometric traits are inherently associated with some specific properties which make them immune to such situations. The principal cause of these benefits is the fact that biometric traits are *something you are*, whereas the token based systems are *something you know*.

1.2 Biometric Traits

Any biometric system is operationally based on one or more biometric traits. These traits or features refer to the physiological and behavioral properties associated with living beings which possess certain characteristics. These are [10] -

- *Universality* - Each subject must possess the specific biometric trait.
- *Distinctiveness* - The biometric trait must be sufficiently distinguishable for any two persons.
- *Permanence* - The biometric trait should not change with time, i.e. it should be time invariant.

- *Collectability* - The trait should be easily collectible from every subject. Preferably, the collection method should be passive.

In addition to these essential requirements, a practical biometric system must also handle some other related issues. These include -

- *Performance* - The achievable recognition accuracy and speed of the system must be satisfying.
- *Acceptability* - The biometric system users must be willing to accept the use of the particular trait.
- *Circumvention* - This is a security paradigm stating that how easily the system can be fooled by impostors.

Examples of some prominent biometric traits which adhere to these properties include fingerprint, face, iris, retina, palmprint, gait, keystroke, signature and voice. The extent to which these traits follow the aforementioned properties is displayed in a tabular form in Table 1.1 [10].

Biometric Trait	**Universality**	**Distinctiveness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
Fingerprint	Medium	High	High	Medium	High	Medium	Medium
Face	High	Low	Medium	High	Low	High	High
Iris	High	High	High	Medium	High	Low	Low
Retina	High	High	Medium	Low	High	Low	Low
Palmprint	Medium	High	High	Medium	High	Medium	Medium
Gait	Medium	Low	Low	High	Low	High	Medium
Keystroke	Low	Low	Low	Medium	Low	Medium	Medium
Signature	Low	Low	Low	High	Low	High	High
Voice	Medium	Low	Low	Medium	Low	High	High

TABLE 1.1: Comparison of various biometric trait in terms of the essential required properties.

The presented biometric traits, however, does not always stringently follow these requirements. For examples, it has been observed and reported that individually, a single biometric trait cannot satisfy all the required characteristics mentioned previously [11]. To overcome these and more problems, the concept of multimodal biometrics was introduced. A multimodal biometrics system utilizes more than one biometric trait for recognition and verification purposes. Although the application of this novel idea mitigated some difficulties associated with the unimodal systems, some new problems came to the forefront. Especially, the *cost* and *verification time* significantly increased since the multimodal framework utilizes more than one modality.

1.3 Biometric System Features

1.3.1 System Modules

A biometric system is essentially a pattern recognition system based on biometric traits. Such a typical framework consists of four distinct modules, each of which is designed for a specific purpose. On an abstract level, these modules are termed as - (i) sensor, (ii) feature extractor, (iii) system database and (iv) matcher. The functionality of each module is described below.

- **Sensor** - The sensor is the input module of the biometric system which captures the biometric samples in their raw format.

- **Feature extractor** - This module is used for extracting discriminating features from the raw biometric data. Comparisons between two biometric samples are performed on the basis of this extracted data.

- **Database** - The output of the feature extraction module gets stored in a stable database. This database can be kept either locally or in a centralized manner.

- **Matcher** - This final module facilitates in the matching procedure of the biometric samples, thereby generating some relevant score. The final decision is taken based on this score and a threshold.

1.3.2 Operation Modes

A typical biometric system works in two modes, namely *enrollment* and *authentication*. In the enrollment phase, biometric traits are collected from individuals and accumulated in a database. On the other hand, users present their query biometric samples for matching purposes in the authentication phase. Based on the system requirements, the authentication phase can be further subdivided into *identification* and *verification* phases. In the identification procedure, a querying individual provides only his/her biometric sample to the system without claiming any identity. The presented sample is subsequently matched with all the samples stored in the database. A single match in between the samples is enough for the system to declare the user as genuine. In certain implementations, the system generates a list of candidate identities from the database ordered according to their similarity to the query.

The biometric templates stored against the candidate identities are then manually matched with the query to identify the true match. The whole identification process is often referred to as a 'one-to-many' search and is primarily used for identifying listed criminals and for government aided registration systems (e.g. voting id) [10]. Perhaps the most prominent example of this system is the UID system by the Government of India [12] (commonly known as the 'Aadhaar' project) wherein multiple biometric traits were collected for individuals and subsequently a 12-digit unique identity number called Aadhaar was generated.

Alternatively, the verification phase consists of a 'one-to-one' match where the querying user presents an identity claim along-with the biometric sample. The system database is first searched based on the claimed identity. The biometric sample which is indexed corresponding to this identity is then extracted from the database and subsequently matched with the query sample. The system declares a match if the matching score is greater than a predefined threshold and declares a non-match, otherwise. A successful matching or authentication renders the user as a genuine entity and consequently is granted permissions for accessing any other applications. Most of the commercial biometric recognition systems operate in verification mode where the user is asked for an identification number before matching. The various operation modes of a biometric recognition system are schematically illustrated in Figure 1.3.

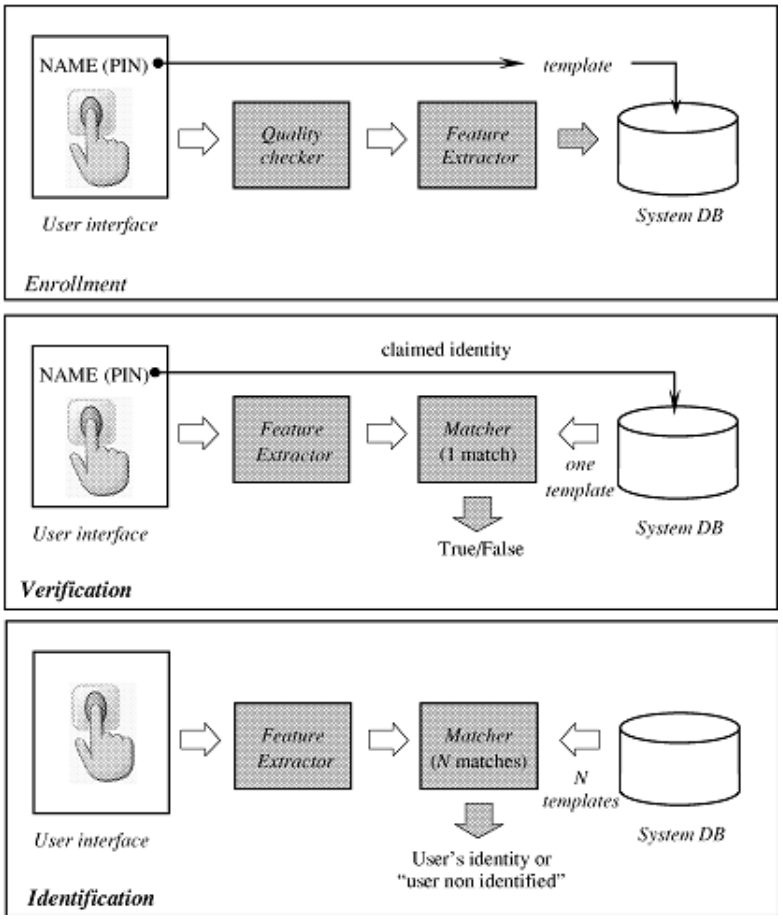

FIGURE 1.3: Different working modes of a biometric system.

1.4 Application Domains

Biometric recognition systems have a wide range of applications. From forensic investigations to access control (e.g. computer log-in), biometric systems are ubiquitous. Broadly speaking, the application areas can be divided into *commercial*, *government* and *forensic*. These are explained as following -

- **Commercial** - Commercial applications essentially relate to the industrial utilities. Typical uses of biometric systems include computer network login,

electronic data security, e-commerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, and distance learning.

- **Government** - Biometric systems are also reliably employed by national governments. Such applications consist of national ID card, correctional facility, driving license, social security, welfare disbursement, border control, and passport control.

- **Forensic** - Forensic denote the study of scientific methods and techniques for investigations related to crime. Biometric applications in this domain comprise of corpse identification, criminal investigation, terrorist identification, parenthood determination and missing children.

1.5 Performance Measures

The central aspect to evaluate the performance of a biometric system is its accuracy. From a user's perspective, an error of recognition occurs either when the system fails to authenticate the identity of a registered person, or when the system erroneously authenticates the identity of an intruder. A major limitation of biometric systems is related with the intra-class variation of biometric samples. More specifically speaking, two biometric samples obtained from a single person but under different conditions (mainly temporal) differs considerably. This discrepancy occurs due to a variety of reasons including imperfect imaging conditions (e.g., sensor noise and dry

(a) Fingerprint (b) Face

FIGURE 1.4: Intra-sample variations for biometric features.

fingers), changes in the user's physiological or behavioral characteristics (e.g., cuts and bruises on the finger), ambient conditions (e.g., temperature and humidity), and user's interaction with the sensor (e.g., finger placement). This undesirable property is pictorially illustrated in Figure 1.4 for fingerprints and facial images. The ultimate objective of any biometric systems is to incorporate some mechanism for reducing the intra-class variations, while simultaneously increasing the inter-class (samples obtained from different persons) variations.

1.5.1 Score Distributions

A matching algorithm of biometric systems comprises of two essential steps. In the first step, an evaluation process assigns a similarity score to the comparison. That similarity score is a value typically in the range $[0 - 1]$; a higher value of score indicates more similarity between samples. The second step decides if the comparison is genuine or impostor by using a frontier threshold or decision threshold (DT). If the score is higher than the threshold, the algorithm decides it is a genuine comparison. Alternatively, a matching process generating a score lower than DT is

deemed as an impostor attempt. Importantly, the decision threshold can be tuned by algorithm users to obtain optimized results corresponding to some specific settings.

Statistical techniques are used to estimate the confidence of that matching algorithm. Initially, it is tested on a very large set of comparisons for which the actual type (genuine, impostor) is known in advance. For each different score value in range $[0 - 1]$, the number of genuine and impostor comparisons that has been assigned that score value (i.e., the frequency of each score value on the set of genuine and impostor comparisons) are computed separately. Those quantities are subsequently plotted separately as two functions for genuine and impostor score distribution. A typical score distribution for a real world matching algorithm is shown in Figure 1.5.

1.5.2 System Errors

The score distribution functions are good tools for the analysis of score behavior but not for algorithm error behavior. Therefore, the biometric community defines two principal cumulative distribution functions for error analysis. They are -

- **False Matching Rate (FMR)/False Accept Rate (FAR)** - This error rate measures the percent of invalid inputs that are incorrectly accepted. Thus the algorithm erroneously classifies an actual impostor comparison as genuine.
- **False Non Matching Rate (FNMR)/False Reject Rate (FRR)** - This metric measures the percent of valid inputs that are incorrectly rejected.

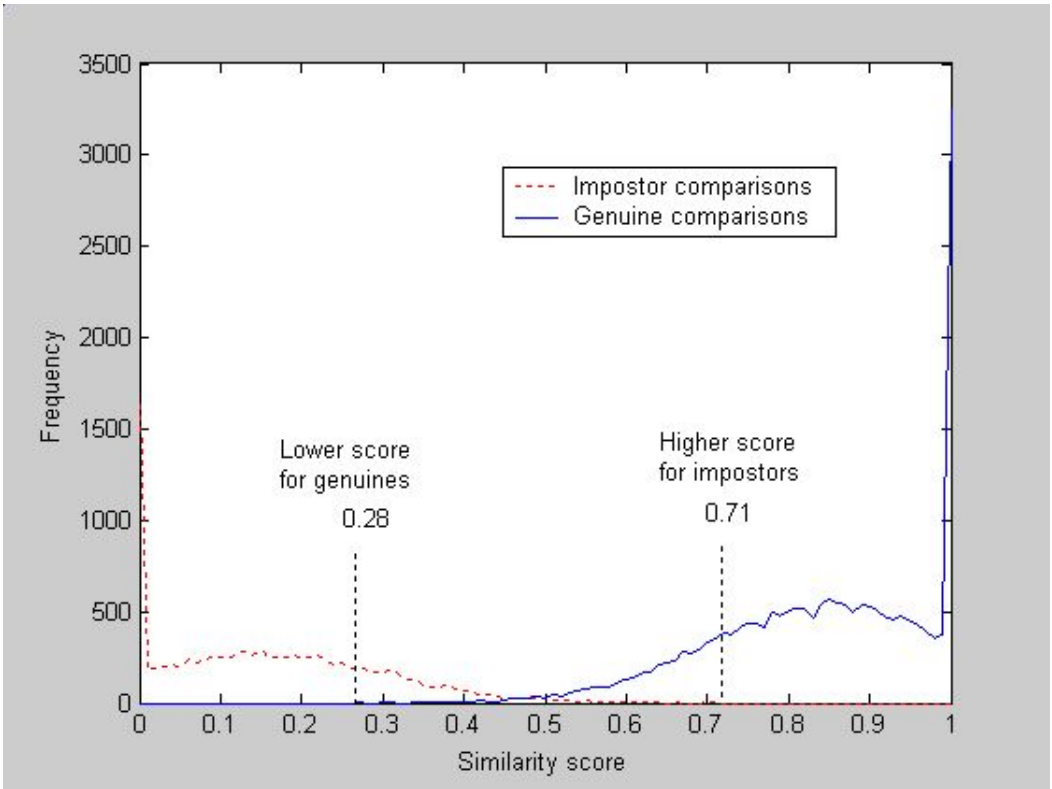

FIGURE 1.5: Score distribution for a real matching algorithm. Impostor comparison scores are distributed on range [0 , 0.71] and genuine comparison scores are distributed on range [0.28 , 1.0]

Herein the algorithm erroneously classifies an actual genuine comparison as an impostor. A related metric to FRR is the **Genuine Accept Rate (GAR)**. It is defined as - $GAR = 1 - FRR$.

The FAR and FRR functions corresponding to Figure 1.5 are shown in Figure 1.6.

Apart from FMR and FNMR, there are several other utility metrics for depicting and visualizing the overall performance of biometric systems. One of the most important parameters for indicating the recognition accuracy of a biometric system is the **Equal Error Rate (EER)**. It is the value where FMR and FNMR are equal at a certain threshold. EER is the single best description of the error rate of

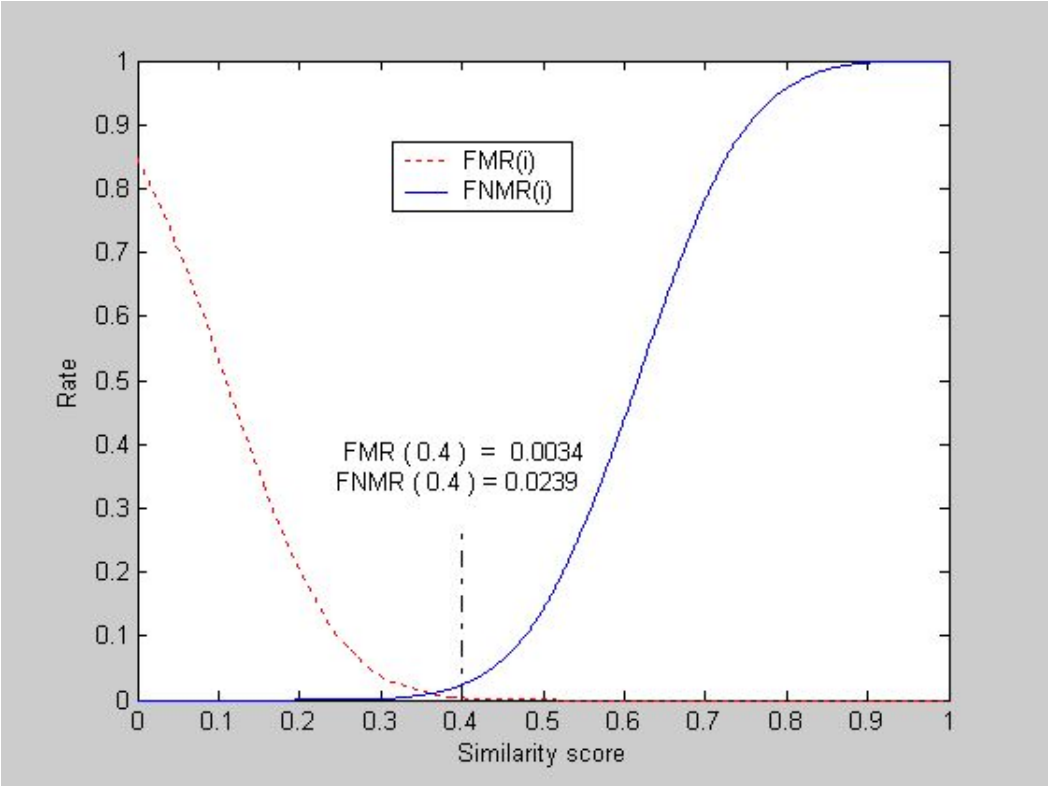

FIGURE 1.6: FMR and FNMR function distributions. For the score of 0.4, the FMR and FNMR are respectively 0.0034 and 0.0239.

an algorithm; a low value of EER translates to lower error rates of the algorithm (which is desirable) and vice versa.

The EER depicts a meaningful but restricted set of pairs (FMR,FNMR). For a more detailed analysis of error behavior, all the (FMR,FNMR) combinations must be considered. The **ROC (Receiver Operating Characteristic)** function is the best way to describe the (FMR,FNMR) variation. In the ROC function, all the pairs of related values of FMR and GAR are plotted together without information about the score. Hence it presents a visual characterization of the trade-off between the two error rates. A sample ROC curve is illustrated in Figure 1.7. The best possible performance of a biometric system would yield a point in the upper left corner

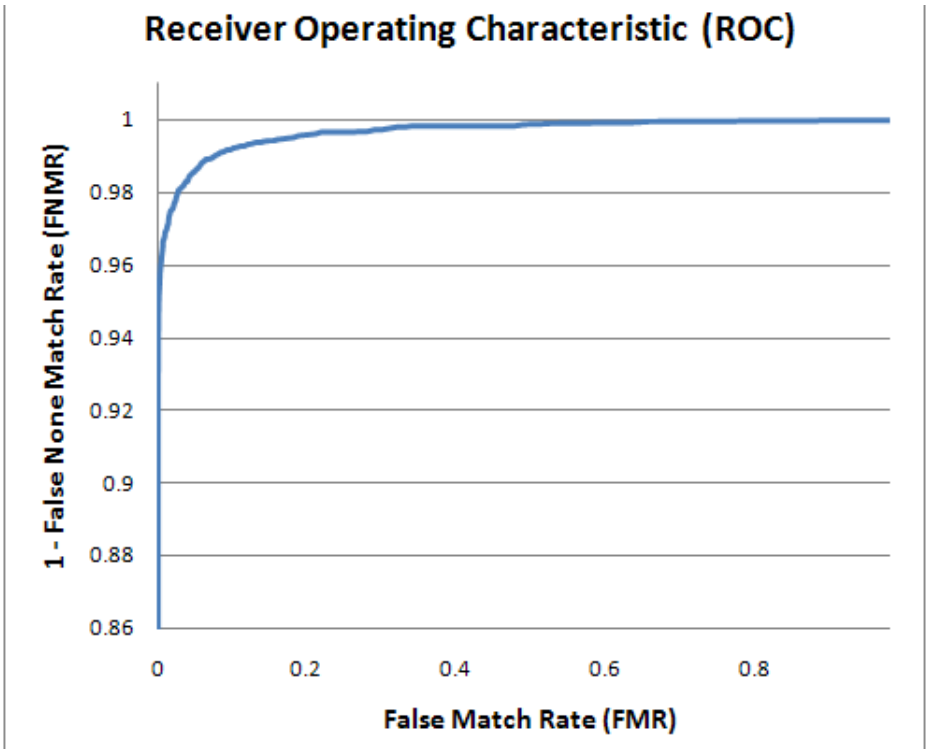

FIGURE 1.7: Demonstration of a ROC curve.

or coordinate (0,1) of the ROC space, which consequently indicates zero incorrect matches (both genuine and impostor).

All of the errors discussed till now are induced due to the misclassification of the biometric recognition process. However, there are several types of errors which are caused owing to other aspects of the system like sensors and human intervention. The most prominent examples of these circumstantial errors include the **Failure To Capture (FTC)** rate and the **Failure To Enroll (FTE)** rate. The FTC error denotes the percentage of times the biometric device (i.e. sensor) fails to capture a sample when the biometric sample is presented to it. This type of errors generally occurs when the sensor is not able to locate a biometric signal of sufficient quality (e.g. poor image quality). Alternatively, the FTE error indicates the percentage of

time the subjects are unable to enroll in the biometric system. The FTE arises when the extracted features from the raw biometric data are of extremely low quality. A high value of FTC and FTE errors normally indicate that there is some problem with either the input sensors or the biometric subjects themselves. Nevertheless, a high value for both these error rates also helps in maintaining a good quality of stored biometric templates and consequently the overall system accuracy improves.

1.6 Attacks on Biometric Systems

A generic biometric system has numerous vulnerabilities and security issues associated with it [13]. In this context, it is first imperative to formally define few terms. The primary step in analyzing the security of any system is to define a *threat model*. The threat model itself can be completely described regarding *threat agent* and *attack model*.

1.6.1 Threat Agent

In general, a threat agent can be defined as a person or a thing that has the power to subvert the intended operation of a system. In terms of biometric models, the threat agent can be of two types - *intrinsic* and *adversarial*. These are explained as

-

- **Intrinsic** threats are caused due to the intrinsic limitations of the system itself. As discussed previously, all biometric systems are prone to various types of internal errors such as FAR, FRR, FTE and FTC. These errors are caused due to the intrinsic limitations of various modules in a biometric system like sensor, feature extractor, and matcher. These failures are also known as *zero-effort attacks* since there is no involvement of any adversary herein.

- **Adversarial** threats are the more conventional modes of biometric system failures. These threats are caused by the presence of an active or passive adversary in the system. The adversaries themselves may be either internal (belonging within the system like system administrators) or external (belonging outside the system like impostors). [1]

1.6.2 Attack Model

Another facet for analyzing the security aspects of biometric systems is to describe the associated *attack model*. An attack/threat model refers to the actual mechanism or path that can be used to circumvent a biometric system. The various classifications of the biometric system attack model are illustrated in Figure 1.8 along-with the specific attacks. Based on the attack agent, the attack mechanisms are divided into *intrinsic failure* and *adversarial attacks*.

[1] In the biometric context, the term impostor refers to any individual who intentionally or inadvertently tries to impersonate another enrolled person.

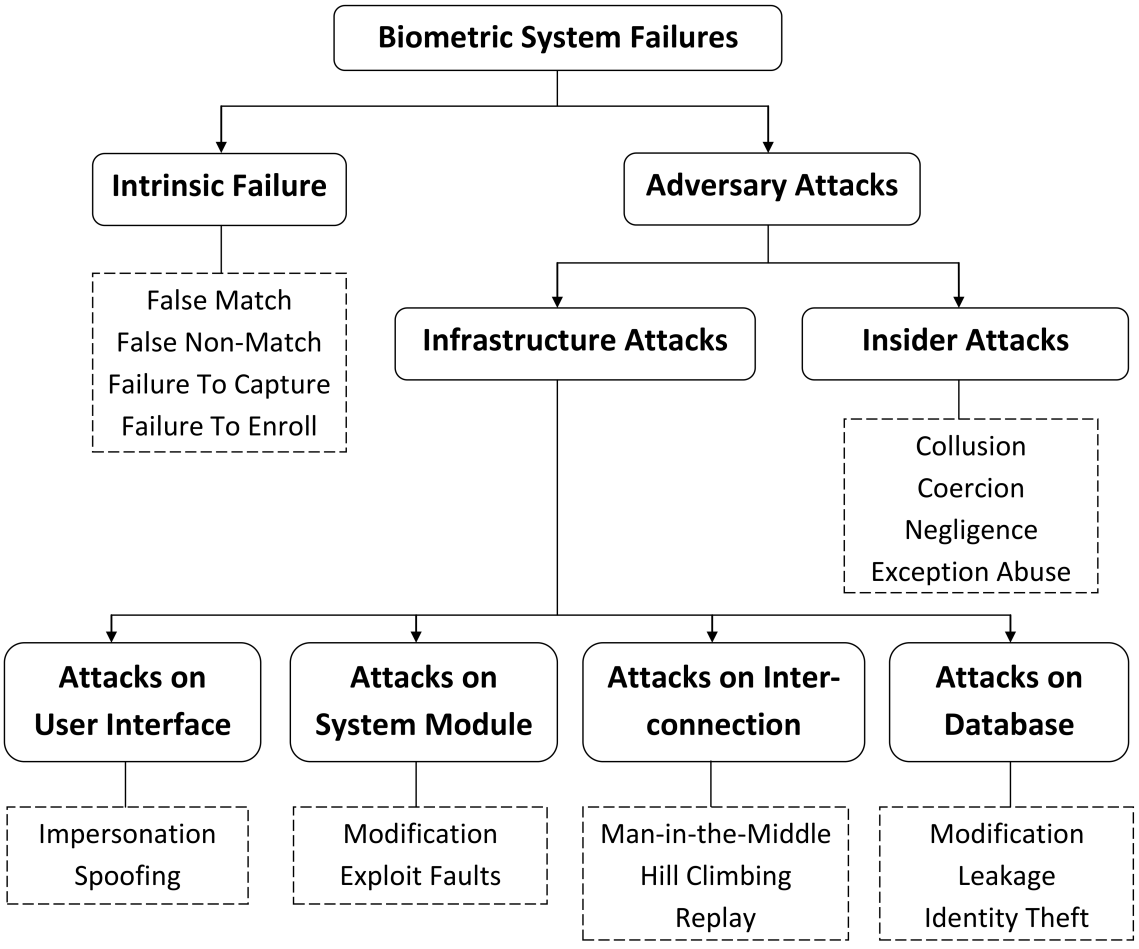

FIGURE 1.8: The biometric system attack model.

Intrinsic failures are caused by the intrinsic agents, i.e. internal errors such as FAR, FRR, FTE and FTC. Each one of these factors results in disruptions inside the biometric system in one way or another. For instance, a false non-match error (FRR) will lead to denial-of-service and inconvenience to genuine users, whereas a false match error (FAR) would considerably diminish the recognition accuracy of the model.

1.6.3 Adversary Attacks

Unlike the case of zero-effort attacks, the success of an adversary attack depends on a variety of factors, including implementation and operational details of the biometric system, the resourcefulness of the adversary (e.g. time and computational power constraints), and the behavior of users interacting with the biometric system. An adversary who intends to subvert a biometric system can make use of vulnerabilities either in the human element or the system infrastructure. Based upon the nature of the adversary, these attacks can be categorized as *insider attacks* and *infrastructure attacks*.

1.6.3.1 Insider Attacks

Biometric systems require human interaction at several stages. For instance, an administrator is usually assigned to assist during the enrollment and authentication phases. Additionally, there may be the presence of specialized operators to supervise the proper functioning of the biometric system and to guide the users. Finally, there are the end users of the biometric system who access applications or resources after authenticating themselves by it. These human interactions can be exploited in several ways for the purpose of breaching the security of the system. Some of these attack scenarios are briefly described below.

- **Collusion** - Collusion refers to the situation when a genuine user voluntarily turns malicious and attacks the system. The attack can be carried out either individually, or in collaboration with other external forces.

- **Coercion** - This situation is similar to collusion, except that the user is forced to carry out the attacks. Nonetheless, it's end result is the same, i.e. security breach of the biometric system.

- **Negligence** - As the name suggests, negligence of authorized users causes these type of attack scenarios. The most common example of negligence is observed when the authorized users carelessly forget to log-out from the system after a successful session.

- **Exception Abuse** - A typical biometric system incorporates a fall-back mechanism to permit handling of exceptional situations (if encountered). An adversary can sometimes utilize this exception handling mechanism and exploit any loopholes of the system.

1.6.3.2 Infrastructure Attacks

Infrastructure attacks are the most common forms of adversarial threats encountered by a biometric system. These attacks are targeted at the various vulnerable modules of the system. A high level schematic diagram is presented in Figure 1.9 which illustrates the various forms of infrastructure based attacks encountered in each module.

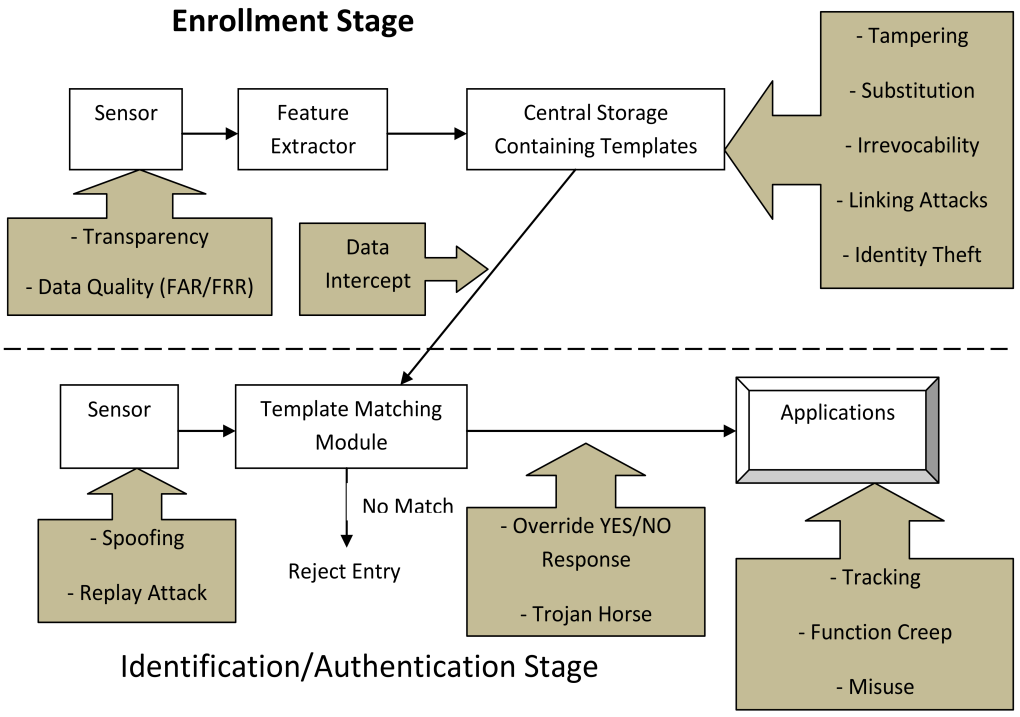

FIGURE 1.9: Various forms of infrastructure based attacks.

On the basis of the targeted module, attacks against the biometric infrastructure can be categorized into four main groups-

- **Attacks at user interface** - The user interface of a biometric system consists of a sensor which captures biometric signals in digital form from enrolling users. An adversary might try to circumvent this module by either damaging the sensor hardware or by masquerading as a genuine user via presenting spoofed biometric samples. While making the sensors robust partially solves the first problem, preventing spoofing attacks is far more complicated. However, modern sensors are usually equipped with liveness detection techniques for discriminating fake samples from original ones.

- **Attacks at interconnections** - An active adversary might try to mount a *man-in-the-middle* attack to intercept and replace data from the interconnection between the various modules. In this common form of attack, the adversary maintains separate connections between multiple modules of the framework and relays messages between them. However, the modules themselves assume that they are directly communicating with each other without any external intervention. These types of attacks serve a dual purpose of revealing personal information and heavily degrading the system performance.

- **Attacks on software modules** - An adversary can potentially alter a software module by injecting a computer virus or a trojan horse. Although created for different purposes, these malicious pieces of codes achieve the common goal of performing hazardous tasks in disguise. For instance, trojan horse codes are often used to bypass the system modules and directly inject the raw user data into the database, whereas a computer virus can force the module to output false values as desired by the adversary.

- **Attacks on the template database** - This is by far the most severe form of adversarial attack on biometric systems. A successful attack on the biometric database poses several hazardous prospects for the system users. Common attack techniques such as tampering and template substitution are very much possible if the database gets compromised in any way. In the worst case, the adversary might steal the genuine user's biometric information and misuse it to access other applications in which the user had previously enrolled. This

type of extremely dangerous prospect is known as *identity theft*. The issue of privacy is also very much relevant in this form of attack. A resourceful adversary might try to link the acquired biometric data of a user with other external sources of data, thereby mining sensitive information about the user.

1.7 Objectives of the Thesis

This dissertation is dedicated towards the development of novel schemes for countering against adversarial attacks on the biometric template database. A general solution to the problem of biometric data security is to store some *appropriate* data associated with the biometric samples, instead of actually storing them. This can be represented by an encoding function -

$$Enc : B \rightarrow B'$$

Here B is the original biometric data and B' is the actual data that gets stored in the database.

As elaborated in later chapters, the notion of *biometric cancelability* is employed as the underlying design principle for the proposed frameworks in this dissertation. Under this paradigm, the original biometric signals are deliberately modified with the aid of a distortion parameter (derived from a user specific key) to produce a transformed template. The alteration process must be carried out by a specialized

function which is very hard to invert under normal conditions (i.e. one-way). The essence of *cancelable biometric* schemes lie in the fact that the stored template (B') can be replaced by another transformed form (say B'') in case B' gets compromised. Regeneration of B'' would entirely depend on the distortion parameter.

A major problem with cancelable biometric schemes is that the overall performance of the resulting biometric recognition system degrades. This deterioration in performance occurs since matching between two biometric templates occur in the transformed space, rather than in their basic forms. As such, another vital goal of this dissertation is designing cancelable schemes which do not diminish the recognition accuracy rates of the biometric system. Thus these techniques would have the dual advantage of strong security guarantees along-with acceptable performance measures.

The final aspect of this thesis is related to soft biometric traits. As already discussed, soft biometric traits are ancillary properties which assist in the biometrics recognition process. Since there exist multiple benefits of using this information, researches in the development of fusion models incorporating soft biometric traits along-with primary ones is very active. However, the security and privacy issues which accompany them have not been adequately addressed in the literature. This study concludes with a formal investigation into the privacy issues associated with soft biometric traits and subsequently attempts to design a suitable privacy preserving multimodal framework for the same.

An underlying intention of this thesis is to develop schemes based on proper cryptographic primitives and notions. The merge of biometrics and cryptography has not been successful due to the nature of the biometric signals. As mentioned previously, biometric samples suffer from the inherent problem of intra-class variations. This undesirable property makes it very difficult to implement standard cryptographic techniques therein. However, if the merging process of cryptography and biometric is made feasible, it would introduce strong security guarantees and provable computational bounds to the system. Subsequently, the various aspects of the resulting frameworks could be rigorously analyzed as well as experimentally vindicated.

All the objectives of this dissertation have been explicitly listed below for clarity:

- Perform a comprehensive literature review of biometric template protection schemes and investigate their strengths and limitations.
- Develop novel schemes which do not result in the degradation of the recognition accuracy rates of the biometric system.
- Design biometric template protection schemes which incorporate cryptographic primitives in them. Accordingly, construct suitable mechanisms for fingerprints and iris based systems.
- Investigate potential privacy issues with soft biometric traits, and accordingly provide mechanisms for preserving the privacy in soft biometric based multimodal fusion frameworks.

1.8 Contributions

Biometric template security is a growing and active area of research. The need and motivation behind such works have been elaborated in the previous discussion. This thesis proposes three novel schemes for providing suitable security measures for fingerprint, iris and soft biometrics based recognition systems. The detailed contributions of this thesis are systematically stated below -

- A comprehensive literature survey of existing biometric template protection scheme is presented. This survey covers the state-of-the-art techniques employing the design principles of both *biometric cryptosystems* and *cancelable biometrics*. The strengths and limitations of these schemes are also investigated, thereby providing right directions for potential novel researches in this area.

- A cancelable scheme for fingerprints is proposed which utilizes cryptographic hash functions. The complete framework is divided into six different modules, each one realizing a specific task. The core of this design consists of cryptographic hash functions (e.g. SHA-256, WHIRLPOOL etc.), which provide strong security guarantees like *non-invertibility* and *collision resistance*.

- A biometric security scheme for iris based systems is proposed. Similar to the previous fingerprint based technique, this framework is also modeled on the notion of cancelable biometrics. The whole framework pivots around the

implementation of adaptive Bloom filters, which are essentially space-efficient probabilistic data structures. They are extensively used to test whether an element is a member of a set or not. The most significant advantages of this approach are non-requirement of any alignment of the iris templates (a sequence of bit known as 'IrisCode') and provable security guarantees.

- Security and privacy issues related to soft biometric traits have been blatantly overlooked in the research community. As such, this problem has been addressed in this thesis by developing a formal model which accurately quantifies the loss of privacy in the event of a leakage in soft biometric databases. This model also describes the roles of other associated privacy defining factors such as 'auxiliary side information' and 'sanitization mechanisms'. Subsequently, a privacy preserving soft biometric based multimodal framework is developed which caters to the aforementioned issues. The popular privacy imparting notion of *differential privacy* is utilized for achieving the desirable objectives.

To briefly summarize the contributions, this thesis presents ad-hoc investigations into the development of secure schemes for biometric templates. The schemes themselves employ a wide variety of concepts like hash functions, perfect secrecy, Bloom filters and differential privacy. One of the primary objectives of this thesis is to justify the use of proper cryptographic definitions in the realm of biometric data, which it achieves successfully.

1.9 Thesis Organization

The rest of the thesis is organized as follows -

Chapter 2 presents a comprehensive survey of biometric template protection schemes. This review work meticulously examines the two main techniques catering to the security needs of biometric data, namely *biometric cryptosystems* and *cancelable biometrics*. Seminal works employing these two design principles are studied along-with their relative strengths and weaknesses.

Chapter 3 presents a robust technique for securing fingerprint based templates. The proposed scheme sequentially employs a directed reference point estimation based pre-alignment process, hexagonal grid based quantization scheme and a cryptographic hash function based transformation for securing minutia points of fingerprints (representing fingerprint traits). Both theoretical and empirical proofs of the security notions are provided in the analysis part of the proposed model.

Chapter 4 introduces a modified Bloom filters based template protection scheme for iris features. The cryptographic notion of *perfect secrecy* is utilized for providing the essential properties of *unlinkability/diversity*, *non-invertibility* and *zero information leakage* in the framework. The proposed scheme is proven to be perfectly secure under the Ciphertext-only Attack (COA) model. Moreover, there is no degradation in the performance measures while employing this technique since the comparison of biometric features is performed in the original space instead of a transformed space.

Chapter 5 essentially addresses the problem of privacy preservation in the context of soft biometric traits. The entire chapter is divided into two parts. While the first part formally establishes the risks ensuing from leaked soft biometric databases (especially during *cross-linking*), the second part proposes a privacy preservation scheme for the same based on the notion of *differential privacy*. As in the case with previous works, both theoretical and experimental analysis are provided for the proposed technique.

Chapter 6 concludes the dissertation along with its potential future enhancements.