Biometric Authentication in Computer Security

[1]Iqbaldeep Kaur, [2]Nafiza Mann, [3]Bhushan, [4]Bharat Verma, [5]Gurbaj
[1,2,3,4,5]Dept. of CSE, Chandigarh Engineering College, Landran, Punjab, India

Abstract
Biometric recognition refers to an automatic recognition of individuals based on feature vector(s) derived from their physiological and/or behavioural characteristic. Biometric recognition systems should provide a reliable personal recognition schemes to either confirm or determine the identity of an individual. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. By using biometrics a person could be identified based on "who she/he is" rather than "what she/he has" (card, token, key) or "what she/he knows" (password, PIN). In this paper, a brief overview of biometric methods, both unimodal and multimodal, and their advantages and disadvantages, will be presented.

Keyword
Biometrics, Multimodal Biometrics, Recognition,Verification, Identification, Security

I. Introduction

The term biometric comes from the Greek words bios (life) and metrikos(measure). It is well known that humans intuitively use some body characteristics such as face, gait or voice to recognize each other. Since, today, a wide variety of applications require reliable verification schemes to confirm the identity of an individual, recognizing humans based on their body characteristics became more and more interesting in emerging technology applications. Traditionally, passwords and ID cards have been used to restrict access to secure systems but these methods can easily be breached and are unreliable. Biometric cannot be borrowed, stolen, or forgotten, and forging one is practically impossible.

One of the oldest and most basic examples of a characteristic that is used for recognition by humans is the face. Since the beginning of civilization, humans have used faces to identify known (familiar) and unknown (unfamiliar) individuals. This simple task became increasingly more challenging as populations increased and as more convenient methods of travel introduced many new individuals into- once small communities. The concept of human-to-human recognition is also seen in behavioural-predominant biometrics such as speaker and gait recognition. Individuals use these characteristics, somewhat unconsciously, to recognize known individuals on a day-to-day basis.

II. Biometrics History

The history of civilization as a more formal means of recognition. Some examples are:

- In a cave estimated to be at least 31,000 years old, the walls are adorned with paintings believed to be created by prehistoric men who lived there. Surrounding these paintings are numerous handprints that are felt to "have…acted as an un-forgeable signature" of its originator.
- There is also evidence that fingerprints were used as a person's mark as early as 500 B.C. "Babylonian business transactions are recorded in clay tablets that include fingerprints."
- Joao de Barros, a Spanish explorer and writer, wrote that early Chinese merchants used fingerprints to settle business transactions. Chinese parents also used fingerprints and footprints to differentiate children from one another.

In early Egyptian history, traders were identified by their physical descriptors to differentiate between trusted traders of known reputation and previous successful transactions, and those new to the market.

By the mid-1800s, with the rapid growth of cities due to the industrial revolution and more productive farming, there was a formally recognized need to identify people. Merchants and authorities were faced with increasingly larger and more mobile populations and could no longer rely solely on their own experiences and local knowledge. Influenced by the writings of Jeremy Bentham and other Utilitarian thinkers, the courts of this period began to codify concepts of justice that endure with us to this day. Most notably, justice systems sought to treat first time offenders more leniently and repeat offenders more harshly. This created a need for a formal system that recorded offenses along with measured identity traits of the offender. The first of two approaches was the Bertillon system of measuring various body dimensions, which originated in France. These measurements were written on cards that could be sorted by height, arm length or any other parameter. This field was called anthropometrics. The other approach was the formal use of fingerprints by police departments. This process emerged in South America, Asia, and Europe. By the late 1800s a method was developed to index fingerprints that provided the ability to retrieve records as Bertillon's method did but that was based on a more individualized metric – fingerprint patterns and ridges. The first such robust system for indexing fingerprints was developed in India by AzizulHaque for Edward Henry, Inspector General of Police, and Bengal, India. This system, called the Henry System, and variations on it are still in use for classifying fingerprints.

Condensed Timeline of Biometrics History

KEY	Iris
Biometrics	Palm
Face	Signature
Fingerprint	Speech
Hand Geometry	Vascular

III. Biometric System

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode:

- In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to one comparison to determine whether the claim is

true or not (e.g., "Does this biometric data belong to Bob?"). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

- In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent single person from using multiple identities [26]. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

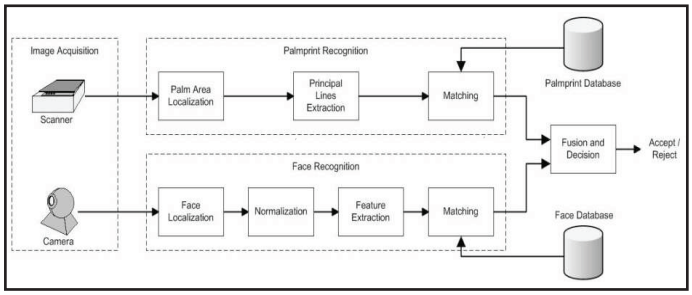


Fig. 1:

The block diagrams of a verification system and an identification system are depicted in fig. 1; user enrolment, which is common to both the tasks is also graphically illustrated.

IV. Biomertic System Errror

Two samples of the same biometric characteristic from the same person (e.g., two impressions of a user's right index finger) are not exactly the same due to imperfect imaging conditions (e.g., sensor noise and dry fingers), changes in the user's physiological or behavioural 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). Therefore, the response of a biometric matching system is the matching score, S(XQ, XI) (typically a single number), that quantifies the similarity between the input and the database template representations (XQ and XI, respectively).

The higher the score, the more certain is the system that the two biometric measurements come from the same person. The system decision is regulated by the threshold, t: pairs of biometric samples generating scores higher than or equal to t are inferred as mate pairs (i.e., belonging to the same person); pairs of biometric samples generating scores lower than t are inferred as non-mate pairs (i.e., belonging to different persons). The distribution of scores generated from pairs of samples from the same person is called the genuine distribution and from different persons is called the impostor distribution (see Fig. 2a).

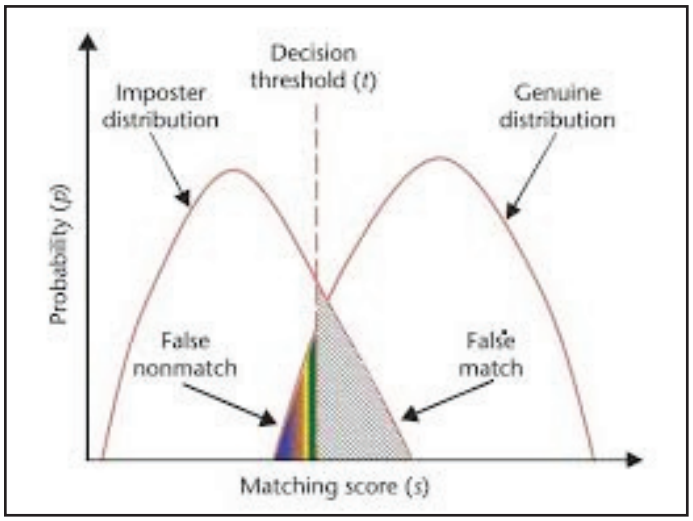


Fig. 2(a):

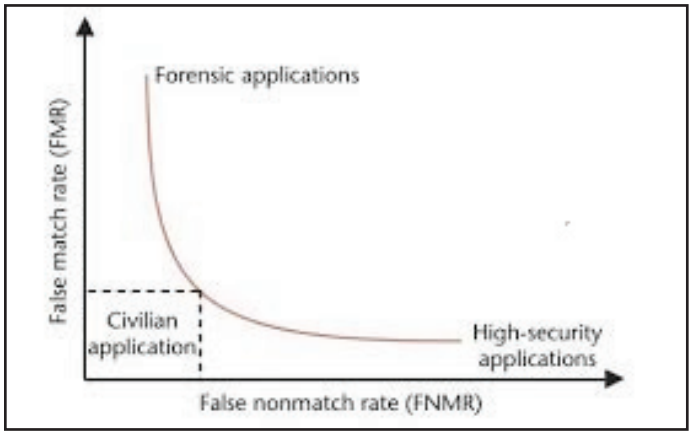


Fig. 2(b):

Fig. 2. Biometric system error rates (a) False match and False non-match for a given threshold t are displayed over the genuine and impostor score distributions; False match is the percentage of non-mate pairs whose matching scores are greater than or equal to t, and False no match is the percentage of mate pairs whose matching scores are less than t. (b) Choosing different operating points results in different False match and False non-match. The curve relating false match to false non-match at different thresholds is referred to as Receiver Operating Characteristics (ROC). Typical operating points of different biometric applications are displayed on an ROC curve. Lack of understanding of the error rates is a primary source of confusion in assessing system accuracy in vendor/user communities alike.

A biometric verification system makes two types of errors: (i) mistaking biometric measurements from two different persons to be from the same person (called false match), and (ii) mistaking two biometric measurements from the same person to be from two different persons (called false non-match). These two types of errors are often termed as false accept and false reject, respectively. There is a trade-off between false match rate (FMR) and false non-match rate (FNMR) in every biometric system. In fact, both FMR and FNMR are functions of the system threshold t; if t is decreased to make the system more tolerant to input variations and noise, then FMR increases. On the other hand, if t is raised to make the system more secure, then FNMR increases accordingly. The system performance at all the operating points (thresholds, t) can be depicted in the form of a Receiver Operating Characteristic (ROC) curve. A ROC curve is a plot of FMR against (1-FNMR) or FNMR for various threshold values, t (see Fig. 2b).

V. A Comparison of Various Biometrics

A number of biometric characteristics exist and are in use in various applications (see fig. 3).

Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is "optimal". The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic. A brief introduction of the commonly used biometrics is given below:

A. DNA

Deoxyribo Nucleic Acid (DNA) is the one-dimensional ultimate unique code for one's individuality - except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. Three issues limit the utility of this biometrics for other applications: (i) contamination and sensitivity: it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose; (ii) automatic real-time recognition issues: the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not geared for on-line non-invasive recognition; (iii) privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g., in hiring practices.

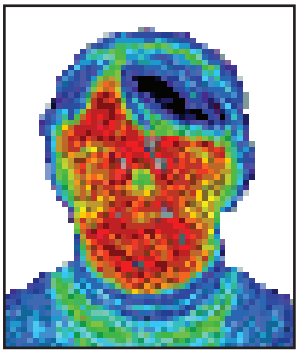
B. EAR

It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

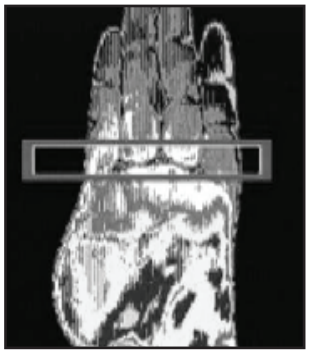
(a)

(b)

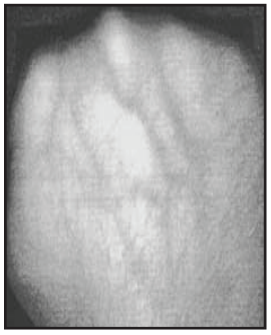
(c)



(d)



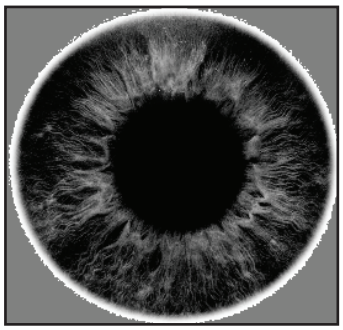
(e)



(f)

(g)

(h)



(i)

Fig. 3: Examples of Biometric Characteristics: a) DNA, b) ear, c) face, d) facial thermo gram, e) hand thermo gram, f)hand vein, g) fingerprint, h) gait, i) hand geometry.

D. Face

Face recognition is a non-intrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled "mug-shot" verification to adynamic, uncontrolled face identification in a cluttered background (e.g., airport). The mostpopular approaches to face recognition are based on either (i) the location and shape official attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatialrelationships, or (ii) the overall (global) analysis of the face image that represents a face asa weighted combination of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available is reasonable [34], theyimpose a number of restrictions on how the facial images are obtained, sometimes requiringa fixed and simple background or special illumination. These systems also have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence [29]. In order that a facial recognition system works well in practice, it should automatically (i) detect whether a face is present in the acquired image; (ii) locate the face if there is one; and (iii) recognize the face from a general viewpoint (i.e., from any pose).

E. Facial, Hand and Hand Vein Infrared Thermo Gram

The pattern of heat radiated by human body is a characteristic of an individual and can be captured by an infrared camera in an unobtrusive way much like a regular (visible spectrum) photograph. The technology could be used for covert recognition. A thermo gram-based system does not require contact and is non-

invasive, but image acquisition is challenging in uncontrolled environments, where heat emanating surfaces (e.g., room heaters and vehicle exhaust pipes) are present in the vicinity of the body. A related technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure. Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermo grams.

F. Fingerprint

Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high [25]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today fingerprint scanner costs about US $20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications. The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification systems involving a few hundred users. Multiple fingerprints millions of identities. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode.

G. Gait

Gait is the peculiar way one walks and is a complex patio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications. Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints or brain, or due to inebriety.

H. Hand and Finger Geometry

Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population.

I. IRIS

The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises(e.g., designer contact lenses). Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective.

VI. Future Trends in Biometrics Security

Biometric technology is one of the most advanced innovations in the digital security industry and today we are going to take a look at three of the most noticeable trends

A. Mobile Biometric Technology

Both governments and the private industry are turning to mobile biometrics to speed up processing of human identification. Mobile biometrics simply means achieving individual biometric identification on a mobile device with the portability to be easily moved or shifted from one place to another. Biometric functionality can be achieved on a mobile device either through its built in biometric sensors or by attaching portable biometric hardware to it via a USB cable or through a Wi-Fi connection.

B. Cloud Based Biometric Solutions

This trend is mainly driven by mobile biometric technology. When you are thinking mobile biometric technology, pairing that mobile biometric device with a cloud based biometric solution can speed up the identification process even more. Instead of saving the biometric data locally, sending it to the cloud is a safer solution.

C. Biometric Single Sign on (SSO)

Perhaps one of the most popular debates at this point is whether biometrics will replace passwords. This debate came to light due to the fact that many companies are adopting biometric single sign on (SSO) over traditional passwords to secure their networks from data breaches and to minimize password management costs. Let's face it, passwords are weak! They are weak because of multiple reasons: they can be guessed, forgotten, shared or swapped. Conversely, biometrics is unique, hard to spoof, and you cannot lose or share them.

VII. Conclusion

Biometrics refers to an automatic recognition of a person based on her behavioral and/or physiological characteristics. Many business applications (e.g. banking) will in future rely on biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made. For instance, fingerprint-based systems have been proven to be very effective in protecting information and resources in a large area of applications. Although companies are using biometrics for authentication in a variety of situations, the industry is still evolving and emerging. At present, the amount of applications employing biometric systems is quite limited, mainly because of the crucial cost-benefit question: supposing biometrics does bring an increase in security, will it be worth the financial cost?

The future probably belongs to multimodal biometric systems as they alleviate a few of the problems observed in uni-model biometric systems. Multimodal biometric systems can integrate information at various levels, the most popular one being fusion at the matching score level. Besides improving matching performance, they also address the problem of no universality and spoofing. Finally, the use of biometrics raises several privacy questions. A sound trade-off between security and privacy may be necessary; but we can only enforce collective accountability and acceptability standards through common legislation [1]. For

example, if and when face recognition technology improves to the point where surveillance cameras can routinely recognize individuals, privacy, as it has existed in the public sphere, will be wiped out. Even today, in some major cities, you are recorded approximately 60 times during the day by various surveillance cameras. IN spite of all this it is certain that biometric-based recognition will have a great influence on the way we conduct our daily business in near future.

References

[1] S. Prabhakar, S. Pankanti, A. K. Jain,"Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, 2003.

[2] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, NY, 2003

[3] A. Eriksson, P. Wretlin,"How Flexible is the Human Voice? A Case Study of Mimicry", Proc. of the European Conference on Speech Technology, pp. 1043-1046, Rhodes, 1997.

[4] W. R. Harrison, Suspect Documents, Their Scientific Examination, Nelson-Hall Publishers, 1981.

[5] D. A. Black,"Forgery above a Genuine Signature", Journal of Criminal Law, Criminology and Police Science, Vol. 50, pp. 585-590, 1962

[6] L. Hong, A. K. Jain, S. Pankanti,"Can multibiometrics improve performance?," in Proc. AutoID'99, Summit, NJ, October 1999, pp. 59-64

[7] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, R. P. W. Duin, "Is independence good for combining classifiers?," In Proc. Int. Conf. Pattern Recognition (ICPR), Vol. 2, Barcelona, Spain, 2001, pp. 168-171

[8] [Online] Available: https://en.wikipedia.org/wiki/Biometrics

[9] [Online] Available: https://en.wikipedia.org/wiki/Fingerprint_recognition

[10] Amit Verma et al.,"Neural Networks: Phoneme Recognition Algorithm", All India Seminar on Emerging Trends in Wireless Communication-Vision 2020 Sponsored by Institute of Engineers, pp.150-156, Held at DIET-Kharar (PUNJAB) on 13th -14th, March 2009.

[11] Amit Verma et al.,"Mobile Agent and IP: Technology For Support of Various Mobile Data", National Conference on Trends in Computing NCTC 2007, pp. 267-273, held at SVIET-BANUR(District Patiala, PUNJAB) on 18th-19th May, 2007.