ISSN:2320-0790

An International Journal of Advanced Computer Technology

Biometric Systems: Evolution, Applications and Technology

[1]Deepti, [2]Dr. Mamta Singhroha, [3]Dr. Virender Kumar

[1]Department of Computer Science & Engineering, NIILM University, Kaithal, Haryana, India

[2]Senior Resident, Department of Radiology, Lady Hardinge Medical College (LHMC), Delhi, India

[3]Senior Resident, Department of Orthopaedics, N. D. M. C. Medical College, Delhi, India

Abstract: Biometrics is a futuristic and yet a current technology, with an ever bigger role in the future. Biometrics will not be able to replace passwords, swipe cards, or pin numbers etc., rather work with them in enhancing security in a simple, reliable, and cost effective way. Biometrics revolution has led to over 1 billion people being already covered by biometric identification programs in the lower middle income countries. Biometric system covers application pertaining to Authentication, Transaction, Access Privilege and it relies on Credentials, Demographics and Sensor data to get a match score with certain degree of confidence using biometric recognition tools. Biometrics systems are extremely useful due to its traits such as security (stop unauthorised person from getting access), convenience (No need to carry credentials like Identity proofs etc.), Audit trail (creates an audit trail for say bank vault access etc.), Fraud prevention (verifying if credit card holder is rightful owner at PoS), and de-duplication (One person, one documentation). India's well known and ambitious pan-India project of Adhaar Card is one good example relying on biometric application for generating unique identification and de-duplication for wide ranging government schemes.

Keywords: Biometrics, Fingerprints, False Acceptance Rate, False Rejection Rate, Authentication Process

I. INTRODUCTION

Biometrics is the technique of using unique, non-transferable, physical characteristics, such as fingerprints, to gain entry for personal identification. This replaces pin codes and passwords, which can be forgotten, lost or stolen. Biometric IDs cannot be transferred.

Biometrics is best defined as measurable physiological and / or behavioral characteristics that can be utilized to verify the identity of an individual. They are of interest in any area where it is important to verify the true identity of an individual. Initially, these techniques were employed primarily in specialist high security applications; however we are now seeing their use and proposed use in a much broader range of public facing situations. Biometrics measure individuals' unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometrics include fingerprints; hand or palm geometry; and retina, iris, or facial characteristics.

II. WHAT IS BIOMETRICS?

Biometrics involves directly the human being for the identification or verification. Traditionally many security systems employ the verification technique rather than the identification, which is the main aim of biometrics. Although it doesn't totally remove the pin/password but with that tool it provide a very tight security system.

Biometrics as said earlier uses the individual's physical characteristics to do its job like hand geometry, retina structure, palm size etc. Biometrics involves different types of devices for doing the same. E.g. fingerprint scanner, iris reader etc. It makes use of the genetic differences between two persons which is a universal truth. Every human being on the earth has a unique identification and that is evident in their different body organs. Biometrics picks up that particular peculiarity to distinguish the two bodies, and that makes it so strong.

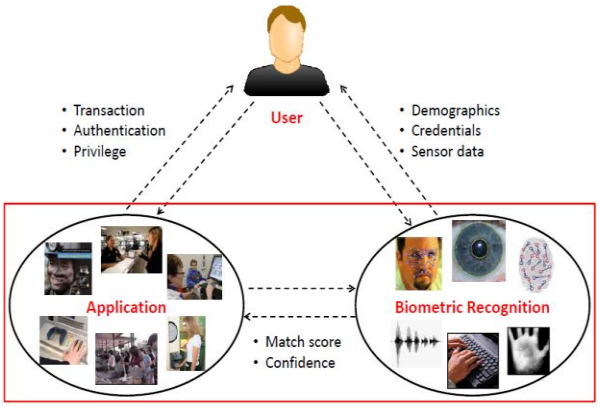

Fig. 1. The Biometrics Conundrum

III. History Behind Biometric Security

In fact, the basic principles of biometric verification were understood and practiced somewhat earlier. Thousands of years earlier to be precise, as our friends in the Nile valley routinely employed biometric verification in a number of everyday business situations. There are many references to individuals being formally identified via unique physiological parameters such as scars, measured physical criteria or a combination of features such as complexion, eye colour, and height and so on.

It is well known that some personnel traits are distinct to each individual and so people can be identified on the basis of their physical characteristics. Of course, they didn't have automated electronic biometric readers and computer networks (as far as we know), and they certainly were not dealing with the large numbers of individuals that we have to accommodate today, but the basic principles were similar.

Alphonse Bertillon, Chief of the criminal identification division, police department in France, Paris developed a detail method of identification based on the number of bodily measurements and physical descriptions. The Bertillon method of anthropometric identification gained wide acceptance before finger print identification superseded it .However such recognition is not limited to faces. For example friends or relatives talking on telephone recognize each other's voices.

Later, in the nineteenth century there was a peak of interest as researchers into criminology attempted to relate physical features and characteristics with criminal tendencies. This resulted in a variety of measuring devices being produced and a huge amount of data being collected. The results were not conclusive but the idea of measuring individual physical characteristics seemed to stick and the parallel development of fingerprinting became the international methodology among police forces for identity verification as most popular method.

Evolution of Biometric sensors over the decades has been captured in the figure below:

Fig. 2. Evolution of Biometric Sensors

IV. Methodologies of Biometrics

A. Retina

An established technology where the unique patterns of the retina are scanned by a low intensity light source via an optical coupler. It involves analyzing the layer of blood vessels situated at the back of the eye. Retinal scanning has proved to be quite accurate in use but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you are a spectacle wearer or have concerns about intimate contact with the reading device. For these reasons retinal scanning has a few user acceptance problems although the technology itself can work well.

B. Iris

An iris-based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil. Iris scanning, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional CCD camera element and requires no close contact between the user and the reader. In addition, it has the potential for higher than average template-matching performance. Iris biometrics work with glasses in place and is one of the few devices that can work well in identification mode. Ease of use and system integration have not traditionally been strong points with iris scanning devices, but you can expect improvements in these areas as new products emerge.

C. Face

A technique which has attracted considerable interest and whose capabilities have often been misunderstood. Face recognition analyses facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. It is one thing to match two static images (all that some systems actually do - not in fact biometrics at all), it is quite another to unobtrusively detect and verify the identity of an individual within a group (as some systems claim). It is easy to understand the attractiveness of facial recognition from the user perspective, but one needs to be realistic in one's expectations of the technology. To date, facial recognition systems have had limited success in practical applications.

D. Signature

Signature verification devices have proved to be reasonably accurate in operation and obviously lend themselves to applications where the signature is an accepted identifier. Signature verification analyses the way a user signs her name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape.
Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to signatures as a means of transaction-related identity verification, and most would see nothing unusual in extending this to encompass biometrics.

E. Voice

Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it requires no new hardware—most PCs already contain a microphone. However, poor quality and ambient noise can affect verification. In addition, the enrolment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly.

Therefore, voice authentication software needs improvement. One day, voice may become an additive technology to finger-scan technology. Because many people see finger scanning as a higher authentication form, voice biometrics will most likely be relegated to replacing or enhancing PINs, passwords, or account names.

F. Hand Recognition

Hand geometry is concerned with measuring the physical characteristics of the users hand and fingers, Hand Geometry scanning systems scan the size, length, thickness and surface of a user's hand (including fingers), in order to verify the user. Unlike other biometrics, such as fingerprints and retina scanning, hand geometry cannot be guaranteed as unique; hence, hand geometry is not an identification technique, but rather a verification technique.

Hand reader machines require the user to first swipe their ID card through the machine, or enter their pin number. Based on the result from this, the hand geometry data for that person is retrieved from a database. The user is then required to place their hand into the reader machine, which has pegs inside to separate the fingers. A scan of the hand is taken and is matched against the hand geometry data retrieved from the database. Assuming the verification is complete, the user is allowed access to the area in question.

G. Fingerprint Verification

A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching minutiae; others use straight pattern-matching devices; and still others are a bit more unique, including things like moiré fringe patterns and ultrasonics. Some verification approaches can detect when a live finger is presented; some cannot.

V. How The System Works

Whilst individual biometric devices and systems have their own operating methodology, there are some generalisations one can make as to what typically happens within a biometric systems implementation.

1. **Sample Selection:** Obviously, before we can verify an individual's identity via a biometric we must first capture a sample of the chosen biometric. This 'sample' is referred to as a biometric template and is the reference data against which subsequent samples provided at verification time are compared. A number of samples are usually captured during enrolment (typically three) in order to arrive at a truly representative template via an averaging process. The template is then referenced against an identifier (typically a PIN or card number if used in conjunction with existing access control tokens) in order to recall it ready for comparison with a live sample at the transaction point. The enrolment procedure and quality of the resultant template are critical factors in the overall success of a biometric application.

2. **Template storage** is an area of interest, particularly with large scale applications which may accommodate many thousands of individuals. The possible options are as follows:
a. Store the template within the biometric reader device.
b. Store the template remotely in a central repository.
c. Store the template on a portable token such as a chip card.

Option 1, storing the template within the biometric device has both advantages and disadvantages depending on exactly how it is implemented. The advantage is potentially fast operation as a relatively small number of templates may be stored and manipulated efficiently within the device. In addition, you are not relying on an external process or data link in order to access the template. In some cases, where devices may be networked together directly, it is possible to share templates across the network.

The potential disadvantage is that the templates are somewhat vulnerable and dependent upon the device being both present and functioning correctly. If

anything happens to the device, you may need to re-install the template database or possibly re-enrol the user base.

Option 2, storing the templates in a central repository is the option which will naturally occur to IT systems engineers. This may work well in a secure networked environment where there is sufficient operational speed for template retrieval to be invisible to the user.

However, we must bear in mind that with a large number of readers working simultaneously there could be significant data traffic, especially if users are impatient and submit multiple verification attempts. The size of the biometric template itself will have some impact on this, with popular methodologies varying between 9 bytes and 1.5k

Option 3, storing the template on a token. This is an attractive option for two reasons. Firstly, it requires no local or central storage of templates (unless you wish to) and secondly, the user carries their template with them and can use it at any authorised reader position.

However, there are still considerations. If the user is attracted to the scheme because he believes he has effective control and ownership of his own template (a strong selling point in some cases) then you cannot additionally store his template elsewhere in the system. If he subsequently loses or damages his token, then he will need to re-enrol.

3. **Verification:** The verification process requires the user to claim an identity by either entering a PIN or presenting a token, and then verify this claim by providing a live biometric to be compared against the claimed reference template. There will be a resulting match or no match accordingly (the parameters involved will be discussed later under performance measures). A record of this transaction will then be generated and stored, either locally within the device or remotely via a network and host (or indeed both).

4. **Transaction storage:** This is an important area as you will certainly wish to have some sort of secure audit trail with respect to the use of your system. Some devices will store a limited number of transactions internally, scrolling over as new transactions are received. This is fine as long as you are confident of retrieving all such transactions before the buffer fills up and you start losing them. In practice, this is unlikely to be a problem unless you have severe network errors.

VI. PERFORMANCE MEASURES

False accepts, false rejects, equal error rates, enrolment and verification times - these are the typical performance measures quoted by device vendors (how they arrived at them is another matter). But what do they really mean? Are these performance statistics actually realized in real systems implementations? Can we accept them with any degree of confidence?

False accept rates (FAR) indicate the likelihood that an impostor may be falsely accepted by the system.

False reject rates (FRR) indicate the likelihood that the genuine user may be rejected by the system. This measure of template matching can often be manipulated by the setting of a threshold, which will bias the device towards one situation or the other. Hence one may bias the device towards a larger number of false accepts but a smaller number of false rejects (user friendly) or a larger number of false rejects but a smaller number of false accepts (user unfriendly), the two parameters being mutually exclusive.

These measures are expressed in percentage (of error transactions) terms, with an equal error rate of somewhere around 0.1% being a typical figure. However, the quoted figures for a given device may not be realized in practice for a number of reasons. These will include user discipline, familiarity with the device, user stress, individual device condition, the user interface, speed of response and other variables.

Accuracy

There are two parameters to judge the accuracy of the biometrics system: false acceptance rate and false-rejection rate. Both methods focus on the system's ability to allow limited entry to authorized users. However, these measures can vary significantly, depending on how you adjust the sensitivity of the mechanism that matches the biometric.

For example, you can require a tighter match between the measurements of hand geometry and the user's template (increase the sensitivity). This will probably decrease the false-acceptance rate, but at the same time can increase the false-rejection rate. So be careful to understand how vendors arrive at quoted values of FAR and FRR.

VII. COMPARISON OF BIOMETRIC TECHNIQUES

Before dwelling into comparing various biometric techniques, let us take a look at the key advantages and disadvantages of a biometric security solution in general.

A. Advantages

Key advantages of biometric solutions include:

- Biometric identification provide a unique identification.

- Biometrics is more reliable and efficient in distinguishing between a specific individual and an imposter.
- Biometric identification protects customers against theft and fraud.
- Identification of the individuals is based on the individual's unique physical and biological qualities that cannot be traded, shared, lost or stolen.
- Degree of the efficiency is too much in the biometric technique.
- The techniques like DNA profiling are highly reliable and efficient that's why it is going to be adopted widely.
- It is much efficient than the (PIN) personal identification number or token-based authentication techniques.
- Key driver for its higher efficiency is that after all it can't be forgotten or lost.

B. Disadvantages

Key disadvantages of biometric solutions include:

- Biometric system may not provide an accurate identification at all times.
- A Biometric system can establish an identity only to a certain level of accuracy.
- FAR (False acceptance rate) is probability by which system can accept imposter as genuine individual.
- FRR (false rejection rate) is probability by which system can reject a genuine individual.
- Cost of the implementation tools is too high (such as finger print sensors are extremely expensive).
- The cost of the storing biometric templates and of the computing power required to process and match biometric measurement is quite high.
- There are some techniques like DNA profiling which are complicated and time taking process.
- Change of hair style in facial recognition, wearing glasses, and light intensity in retina scanning may affect the authentication process.

Table 1 & 2: Comparison of Biometric Techniques

Characteristic	Fingerprints	Hand Geometry	Retina
Ease of Use	High	High	Low
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses
Accuracy	High	High	Very High
User acceptance	Medium	Medium	Medium
Required security level	High	Medium	High
Long-term stability	High	Medium	High

Characteristic	Iris	Face	Signature	Voice
Ease of Use	Medium	Medium	High	High
Error incidence	Poor Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	Very High	High	High	High
User acceptance	Medium	Medium	Medium	High
Required security level	Very High	Medium	Medium	Medium
Long-term stability	High	Medium	Medium	Medium

VIII. APPLICATIONS

Security systems use biometrics for two basic purposes:

To verify or
To identify users.

Identification tends to be the more difficult of the two uses because a system must search a database of enrolled users to find a match (a one-to-many search).

A. Physical Access:

Today, the primary application of biometrics is in physical security: to control access to secure locations (rooms or buildings). Biometrics are useful for high-volume access control.

For example, biometrics controlled access of 65,000 people during the 1996 Olympic Games, and Disney World uses a fingerprint scanner to verify season-pass holders entering the theme park.

Government – passports, national ID cards, voter cards, driver's licenses, social services, etc;
Transportation – airport security, boarding passes and commercial driver's licenses;
Healthcare – medical insurance cards, patient/employee identity cards;
Financial – bank cards, ATM cards, credit cards and debit cards.

B. Virtual Access:

For a long time, biometric-based network and computer access were areas often discussed but rarely implemented. Analysts see virtual access as the application that will provide the critical mass to move biometrics for network and computer access from the realm of science-fiction devices to regular system components. Passwords are currently the most popular way to protect data on a network.

C. E-Commerce:

E-commerce developers are exploring the use of biometrics and smart cards to more accurately verify a trading party's identity. For example, many banks are interested in this combination to better authenticate customers and ensure nonrepudiation of online banking, trading, and purchasing transactions.

Some are using biometrics to obtain secure services over the telephone through voice authentication. Developed by Nuance Communications, voice authentication systems are currently deployed nationwide by the Home Shopping Network.

D. Other Applications Involve:

Voting systems, where eligible politicians are required to verify their identity during a voting process. This is intended to stop 'proxy' voting where the vote may not go as expected.

Junior school areas where (mostly in America) problems had been experienced with children being either molested or kidnapped.
The application of biometrics in near future will be in ATM Machines where the leading banks will use biometrics as a general means of combating card fraud.

IX. Conclusion and Future Work

At its infancy, current biometric technology is still considered immature to completely replace password and other authentication schemes. Security wise, biometric technology shows vulnerabilities that can be easily exploited for wrongful purposes. Biometrics itself is by nature complicated and distinctively secured to each unique identity. It is the imperfect design of the system and its elements that produces the security holes.

Hence, to achieve higher security performance, the design of biometric system should take into consideration the possible vulnerabilities of the processes and algorithms of the system for the whole life cycle, namely data collection, data transmission, storage, templates comparison and susceptibility of the system to physical human attack.

Few of the observations related to Biometric systems are as follows:
1. **Biometric System**: Almost always embedded in an application
2. **Biometric Trait**: No optimal one, but some are better than others
3. **Matcher Accuracy**: Zero error is neither guaranteed, nor required in most cases
4. **System Evaluation**: Error rates in lab tests are invariably lower than the field error rates on ground
5. **Security**: Biometrics is an effective tool only if implemented well
6. **Biometric Template**: Feature extraction is not a one way function and does require corresponding input
7. **Impact**: Impact is not measurable properly without a perspective on both application and technology

X. References

[1] C. M. Bishop, Pattern Recognition and Machine Learning, Springer, 2007.

[2] R. O. Duda, P. E. Hart, and D. G. Stork, Pattern Classification and Scene Analysis, John Wiley and Sons, New York, 2001.

[3] F. Roli, L. Didaci, and G. L. Marcialis, 'Template co-update in multimodal biometric systems', in Advances in Biometrics, pp. 1194–1202, (2007).

[4] P. J. Flynn, K. W. Bowyer, and P. J. Phillips, 'Assessment of Time Dependency in Face Recognition: An Initial Study', in LNCS 2688, 4th Int'l. Conf. Audio- and Video-Based Biometric Person Authentication (AVBPA 2003), pp. 44–51, Guildford, (2003).

[5] Anil Jain, Michigan State University, '50 years of Biometric Research: Almost Solved, the Unsolved and the Unexplored', 2013.

[6] Corinne Fredouille, Johnny Mari´ethoz, C´edric Jaboulet, Jean Hennebert, Chafik Mokbel, and Fr´ed´eric Bimbot, 'Behavior of a bayesian adaptation method for incremental enrollment in speaker verification', in ICASSP2000 - IEEE International Conference on Acoustics, Speech, and Signal Processing, Istanbul, Turkey, (June 5–9 2000).

[7] X. Jiang and W. Ser, 'Online fingerprint template improvement', IEEE Tran. Pattern Analysis and Machine Intelligence, 24(8), 1121–1126, (2002).

[8] X. Liu, T. Chen, and S. M. Thornton, 'Eigenspace updating for non-stationary process and its application to face recognition', Pattern Recognition, 36(9), 1945–1959, (September 2003).

[9] N. Poh, G. Heusch, and J. Kittler, 'On Combination of Face Authentication Experts by a Mixture of Quality Dependent Fusion Classifiers', in LNCS 4472, Multiple Classifiers System (MCS), pp. 344–356, Prague, (2007).

[10] N. Poh and J. Kittler, 'A Method for Estimating authentication Performance Over Time, with Applications to Face Biometrics', in 12th IAPR Iberoamerican Congress on Pattern Recognition (CIARP), pp. 360–369, Via del Mar-Valparaiso, Chile, (2007).

[11] D. A. Reynolds, T. Quatieri, and R. Dunn, 'Speaker Verification Using Adapted Gaussian Mixture Models', Digital Signal Processing, 10(1–3), 19–41, (2000).

[12] X. Zhu, 'Semi-supervised learning literature survey', online publication, University of Wisconsin-Madison, (2008).