

Biometrics Authentication System

Shwetali S Diwanji

Institute of Management and Computer Studies, University of Mumbai, Thane (West), India

Abstract: Over the last few years a new area of engineering science has been established whose products are likely to create a large market in the near future. It has been called "biometrics". The pioneers of this new domain intend to construct devices which would allow identification of a person on the basis of his/her "biological" characteristics: voice, dynamics of movements, features of face and other parts of the body, retina or iris pattern. Nature has made human beings with different characteristics which may vary from one person to another. Biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. Several important issues must be considered in designing a practical biometric system. First, a user must be enrolled in the system so that his biometric template can be captured. This template is securely stored in a central database or a smart card issued to the user. The template is retrieved when an individual needs to be identified. Depending on the context, a biometric system can operate either in a verification (authentication) or an identification mode. - More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number.^[2] Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

Keywords: authentication, security, dna, fingerprint, retina.

I. INTRODUCTION

There are evidences of biometric uses on human history as early as prehistorically age. Estimated 31000 years old caves are adorned with prehistorically pictures apparently signed by fingerprints stamps of authors. Evidence is the use of fingerprints by Babylonian at 500 B.C. They used to record business transactions on clay tables in which were found fingerprint stamps.

The first reported use of biometrics was related by Portuguese explorer Jiao de Barros in the 14th century. He described the practice of Chinese merchants of stamp children's palm prints and footprint to distinguish from one another

The first real biometric system was created in 1870 by French anthropologist Alphonse Bertillon and turned biometrics a distinguished field of study. He developed an identification system (Bertillon age) based on detailed records of body measurement, physical description and photographs. Despite their imprecise measures and difficulty to apply methodology, the Bertillon age was an important advance on criminal and people identification. It began to fail when it was discovered that many people share the same anthropologic measures.

The first classification method for fingerprints was developed in 1892 by Sir. Francis Galton. The features used by Galton's method were the minutiae that are still used nowadays.

Some years later in 1896, Sir Edward Henry General Inspector of the Bengal police, began to use Galton's method to replace the anthropometrics system for identification of criminals. Henry created a method to classify and store fingerprint that lets a quick searching of records. Later, that method was introduced by Henry in London for the first British fingerprint file.

II. TYPES OF BIOMETRICS

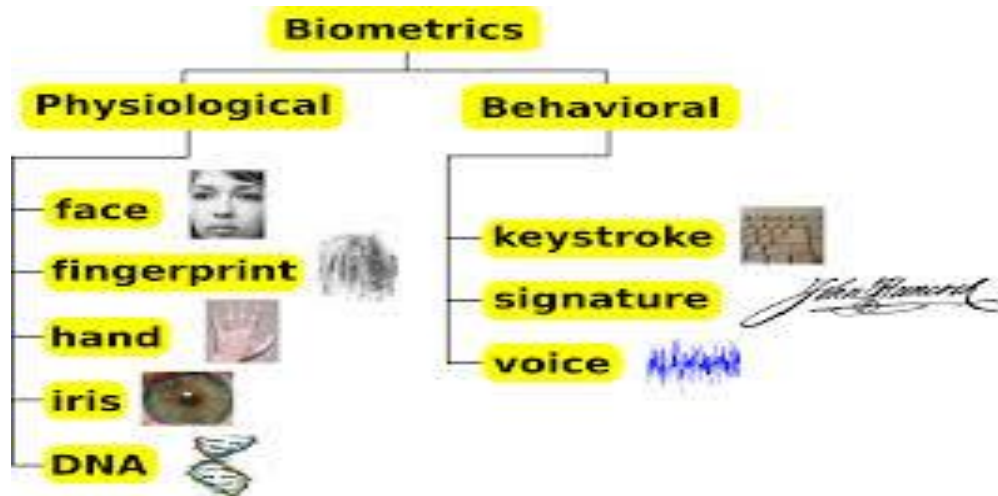


Figure1: basic structure of biometrics system

2:1 Retina scanner - These scan the unique biometric pattern in each person's iris, and match it against a certain number of unique identifying marks that set every person apart from everyone else.

2:2 Iris scanning and retinal scanning are both used to identify a person according to their unique pattern, but they tend to be far costlier and more complex.

2:3 Finger Print Scanner - As far as price goes, the fingerprint scanning is on the lower end of the scale. The cheapest fingerprint scanners are the ones that only scan the actual print, though the costlier ones actually scan the presence of blood in the fingerprint, the size and shape of the thumb, and many other features. These costlier systems actually capture a 3D image of the fingerprint, thereby making it much more difficult for the fingerprint to be counterfeited.

2:4 Facial Biometrics - Each person around the world has a distinctly unique face, even two twins that the human eye cannot tell apart. It may be something as small as the slightly different placing of the eyebrows, the width of the eyes, or the breadth of the nose.

There are certain markers that enable these biometric recognition scanners to instantly identify the uniqueness of each person scanning their facial features, thus enabling the device to ensure that only the single person with the correct bone structure and feature placement can gain access.

2:5 Voice Recognition - Every person in the world has a unique voice pattern, even though the changes are slight and barely noticeable to the human ear. However, with special voice those tiny differences in each person's voice can be noted, tested, and authenticated to only allow access to the person that has the right tone, pitch, and volume of voice. It can be surprisingly effective at differentiating two people who have almost identical voice patterns.

2:6 Hand Print Patterns - When you place your hand on a scanner, you not only have a unique fingerprint pattern, but the size and shape of your entire hand is also very unique.

This includes the width and length of your palm, the width and length of your fingers, the distance between each knuckle, and the depth of each of the lines in your palm. This is more complex than regular fingerprint scanning, and will be much more accurate with less chance of falsification.

III. ADVANTAGES

Biometrics have offered a scalable solution to business owners who are now empowered to circumvent issues like undocumented access, ID swapping, manual badge checks, credential replacements and more.

There have been many developments in the field of biometrics, which means things are more reliable and costs are down. Biometrics offer high level identification management security operations that have several advantages over traditional means and now they are available to you at lower costs.



Many business owners are adopting biometric identification management systems to save money, time, and resources and increase security.

3:1 Accurate Identification:

While traditional security systems are reliant on passwords, personal identification numbers (PINs) or smart cards, you can achieve a high level of accuracy with biometrics systems. If you have set up the system correctly, you can use biological characteristics like fingerprints and iris scans, which offer you unique and accurate identification methods. These features cannot be easily duplicated, which means only the authorized person gets access and you get high level of security.

3:2 Accountability:

Biometric log-ins mean a person can be directly connected to a particular action or an event. In other words, biometrics creates a clear, definable audit trail of transactions or activities. This is especially handy in case of security breaches because you know exactly who is responsible for it. As a result you get true and complete accountability, which cannot be duplicated.

3:3 Easy and Safe for Use:

The good thing about using biometrics for identification is that modern systems are built and designed to be easy and safe to use. Biometrics technology gives you accurate results with minimal invasiveness as a simple scan or a photograph is usually all that's required. Moreover the software and hardware can be easily used and you can have them installed without the need for excessive training.

3:4 Time Saving:

Biometric identification is extremely quick, which is another advantage it has over other traditional security methods. A person can be identified or rejected in a matter of seconds. For those business owners that understand the value of time management the use of this technology can only be beneficial to your office revenue by increasing productivity and reducing costs by eliminating fraud and waste.

3:5 User Friendly Systems:

You can have biometrics systems installed rather easily and after that, they do their job quickly, reliably and uniformly. You will need only a minimum amount of training to get the system operational and there is no need for expensive password administrators. If you use high quality systems, it will also mean your maintenance costs are reduced to minimize the expenses of maintaining an ongoing system.

3:6 Security:

Another advantage these systems have is that they can't be guessed or stolen; hence they will be a long term security solution for your company. The problem with efficient password systems is that there is often a sequence of numbers, letters, and symbols, which makes them difficult to remember on a regular basis. The problem with tokens is that they can be easily stolen or lost – both these traditional methods involve the risk of things being shared. As a result you can't ever

be really sure as to who the real user is. However that won't be the case with biometric characteristics, and you won't have to deal with the problem of sharing, duplication, or fraud.

3:7Convenience:

It's considered to be a convenient security solution because you don't have to remember passwords, or carry extra badges, documents, or ID cards. You are definitely saved the hassle of having to remember passwords frequently or changing cards and badges. People forget passwords and ID cards are lost, which can be a huge nuisance with traditional security methods.

3:8Versatility:

There are different types of biometrics scanners available today and they can be used for various applications. They can be used by companies at security checkpoints including entrances, exits, doorways, and more.

Moreover you can make the most out of the biometric solutions to decide who can access certain systems and networks. Companies can also use them to monitor employee time and attendance, which raises accountability.

3:9Scalability:

Biometrics systems can be quite flexible and easily scalable. You can use higher versions of sensors and security systems based on your requirements. At the lowest level you can use characteristics that are not very discriminative; however if you are looking for a higher level of security for large scale databases then you can use systems with more discriminable features, or multi-modal applications to increase identification accuracy.

3:10Return on Investment:

It's definitely high because you can avoid fraud including "buddy punching," besides lowering payroll costs, accurate calculation of work hours, and reduced management time. While the security is improved you can also easily apply consistent policies and procedures at the same time. And all you have to think about is the initial cost of the biometric system.

You can benefit from biometrics systems to a great extent and do away with the need to remember passwords and combinations. Rather than remembering the password for a computer system or a combination to a safe, you can offer unique biometrics information and get access. The job will be done quickly, accurately, with a fast implementation schedule and minimal training.

IV. CONCLUSION

There are many biometrics devices or we can say that there are many different authentication system:

Proper devices will surely be very useful,

If devices are not proper then there will be a problem,

It has a wide benefit in future,

It has give new life to the field of security.

ACKNOWLEDGEMENT

The Research Work has be supported by IMCOST faculties and biometrics authentication Team. The Research Work has been avidly supported by our college students who iimmensely interested in the field of biometrics

REFERENCES

- [1] J .G Dogman "high confidence visual recognized.
- [2] Parvathi Ambalakat" security of biometrics system.