BIOMETRICS

CONTENTS

ABSTRACT

- This paper basically gives the meaning and origin of the biometrics. It also deals with the identification, operation and the types of biometrics and the fields in which they are used in. It also discusses about the threats and the problems that may be encountered in the due course. Biometric fingerprints are specially discussed here.

INTRODUCTION

- Among many other instances in the animal world, mice and penguins are capable of using their factory senses, aided to some extent by other cues, to very reliably recognize their parents and their progeny, even among large populations packed into a small space. Humans with such capabilities appear to be limited to those whose other senses are severely impaired, such as the blind and deaf Helen Keller (Young 1988). Hence biometric techniques involve 'metrics' or measurements of some kind, rather than depending merely on informal or subliminal methods

- Biometrics is the technique of studying the physical characteristics of a person such as fingerprints, hand geometry, eye structure or voice pattern. Biometrics is an ancient greek word ‘bios’=life, ‘metron’=measure. Biometrics is used for uniquely recognizing humans based on physical traits or behavior traits.

- ❖ Performance of biometric systems is measured in terms of False Accept Rate (FAR), False Reject Rate (FRR).

BIOMETRICSIDENTIFICATION

Research on biometrics began at San Jose State University under the auspices of the College of Engineering in 1994. This study was completed in 1997.The Biometric Consortium established the National Biometric Test Center at San Jose State University in the Spring of 1997. The Test Center has also been carrying out applied research using currently available biometric technologies.

OPERATION

Biometric applications depend on comparing a new measure against a previously captured measure. In order to establish the necessary reference-point, some aspect of a person is measured; the measure may be processed; and the resulting data is stored. At a subsequent time, the same aspect of a person is measured, and compared against the stored data. If it is being used for authentication, the new data is compared against the data already in storage for that person. If it is being used for identification, the entire database is searched, in order to locate one or more individuals that are a close fit to the new data.

Most biometrics technologies do not seek exact equality between the new and the stored measures. Instead they have a pre-set tolerance range within which the two are deemed to be sufficiently close. The biometric measure itself may be stored.

The various forms of identification are: -

- ➢ The identification of products and packaging
- ➢ The identification of vehicles
- ➢ Te identification of animals
- ➢ Forms of identification which show a category to which a person belongs, rather than specifying the individual
- ➢ Te gathering and use of information about identified individuals; and
- ➢ Restrictions on individuals' movements, actions and behavior.

Alternatively the data may be subjected to processing of some kind, and the results of that processing stored instead. The kinds of processing include:

- Compression, in order to reduce transmission time and costs and/or to require less storage space. Compression algorithms are of several different kinds, involving:
  - removal The arbitrary of data;
  - The selective removal of data that has been determined to be of limited value to the matching process between new and stored measures; and/or
  - Te selective inclusion of data that has been determined to be of considerable value to the matching process;
- Encryption, in order to make the data inaccessible to someone who intercepts it in transmission, or accesses it in storage.
- Hashing by which is meant a mathematical conversion that protects the measure from being meaningful to someone who intercepts it in transit. Hashing algorithms are of two kinds:
  - Reversible processes, such that the original measure can be recovered by someone who knows what hashing algorithm was used and

'One-way hash' algorithms, for which no inverse algorithm is known, with the result that the original measure cannot be recovered from the hashed data.

<u>Where can biometrics be used?</u>

Biometrics can be used in almost any application that requires the accurate identification of an individual. This ranges from computers where a fingerprint scan on the mouse can verify the identity of a user to nuclear power plants where various biometrics are used to restrict access to the critical systems.

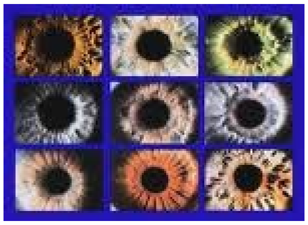
Types of Biometrics

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

Finger Geometry Recognition - Visual/Spatial Biometric The use of 3D geometry of the finger to determine identity.

Face Recognition - Visual Biometric The analysis of facial features or patterns for the authentication or recognition of an individual’s identity. Most face recognition systems either use eigenfaces or local feature analysis.

Eyes - Iris Recognition - Visual Biometric The use of the features found in the iris to identify an individual.



Eyes - Retina Recognition - Visual Biometric The use of patterns of veins in the back of the eye to accomplish recognition

Voice - Speaker Verification - Auditory Biometric The use of the voice as a method of determining the identity of a speaker for access control.

Voice - Speaker Recognition - Auditory Biometric The determination of identity of a speaker use the characteristics of their voice.

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

Signature Recognition - Visual/Behavioral Biometric The authentication of an individual by the analysis of handwriting style, in particular the signature.

Typing Recognition - Behavioral Biometric The use of the **Eyes - Iris Recognition** - Visual Biometric The use of the features found in the iris to identify an individual.unique characteristics of a persons typing for establishing identity.

DNA Matching - Chemical Biometric The identification of an individual using the analysis of segments from DNA.

Ear - Visual Biometric The identification of an individual using the shape of the ear.

Odour - Olfactory Biometric The use of an individual's odor to determine identity.

Gait - Behavioral Biometric The use of an individuals walking style or gait to determine identity.

BIOMTERIC FINGERPRINTS

The electronic data from the two fingerprints is stored in a database and is made available at necessary Department of Homeland Security immigration inspectors. The electronic fingerprint data is associated with an issued visa for verification and the privacy of the data is protected by storage in the database.

The Department of State makes data available in accordance with the law governing the use of visa records, to agencies that require the information for law enforcement purposes.

Where are biometric technologies currently deployed?

Passports:

Research into the use of face recognition for inclusion in passports. Includes significant input into the development of the new international biometric data standards. From 26 October 2005 all newly issued New Zealand and Australian passports used a biometric identifier to continue to meet visa waiver requirements for travel to or through the USA.

Others:

Biometrics is currently being used in the national identification card schemes of both Hong Kong and Malaysia. There are many thousands of biometric deployments around the world too numerous to list here.

IS BIOMETRICS A THREAT TO PRIVACY?

This is a main barrier to wider use of biometric systems. If a person's biometric information is stolen, then their privacy has definitely been breached. However, if certain standards in information collection and protection are met, then biometrics can be a privacy enhancing tool. It is the aim of the Biometrics Institute to see these standards and procedures put in place.

IS THEFT OF A BIOMETRIC POSSIBLE?

A user's biometric cannot be changed like a password. A behavioural biometric such as signature or handwriting cannot be 'stolen' but someone can learn to sign or write like you to a certain extent. A physiological biometric such as fingerprint or face or iris image can be 'stolen' - a copy of raw biometric data (or a feature template) obtained by illegal means. Ideally a biometric is what an individual possesses and another individual should not be able to possess the same. What they have is only a copy of the sensed or measured form of it.

However, merely obtaining the data is not enough. The impostor will have to present the biometric to the system as well and fool the system in this regard. Some systems have "liveness" tests which can reject presentations such as fingerprints copied on plastic material or faces shown as photographs. Clever ways of circumventing such checks have also been devised and there is no completely secure method.

One cannot change a fingerprint if the fingerprint data is stolen - unlike a password. One way to prevent such theft for biometrics such as iris or retinal scans (which cannot be as easily obtained as fingerprints or faces) would be to not supply them in raw form to anyone, but in an encrypted form - what is being referred to as 'cancellable' biometrics. Keys used for encryption and decryption can be changed. It just makes it harder for the thief to get a useful form of the data.

Multimodal systems can have an advantage in this regard. It is more difficult to present the face as well as a fingerprint and sign like another person.

Text-dependent behavioural biometrics are like a combination of password and biometric in this regard. For example, the way you write or speak particular phrases. If someone learns to write like you or mimic your voice for these phrases well, you can change the phrases being used. A random phrase chosen from a large enough vocabulary will make it harder because the impostor will need to learn all the phrases in the vocabulary (which may not even be public). Such systems are referred to as "pseudo-multimodal".

USES OF BIOMETRICS

Biometrics may be used for identification. An example of this is the comparison by police investigators of fingerprints from the scene of a crime against a collection of prints from persons previously convicted of serious criminal offences. In some jurisdictions, government agencies are permitted to collect biometrics without a conviction, or even a charge; and there are increasing attempts to compulsorily or pseudo-voluntarily acquire biometrics from many categories of people only remotely associated with crime (such as visitors to prisons, and people in geographical and/or temporal proximity to the scene of a crime).

Biometrics may be used for authentication. A new measurement that purports to belong to a particular entity is compared against the data stored in relation to that entity. If the measurements match, the assertion that the person is who they say they are is regarded as being authenticated. Some building access schemes work this way, with the system comparing the new measure against the company's employee database.

CONCLUSIONS

Biometrics is one of the most serious among the many technologies of surveillance that are threatening the freedom of individuals and of societies in one possible future, biometrics will fall into ill-repute in relatively free countries. But in authoritarian countries, biometrics will be successfully imposed on the population, resulting in freedoms being reduced even further. Biometrics providers will flourish by selling their technology to repressive governments, and achieve footholds in relatively free countries by looking for soft targets, starting in some cases with animals and in others with captive populations like the frail aged, prisoners, employees, insurance consumers, and welfare recipients. All relatively free countries will become more repressive. Public confidence in corporations and government agencies will spiral much lower. This scenario leads away from freedoms and towards subjugation of the individual to powerful organizations.

It was concluded that organizations should consider whether the nature of their relationships with individuals really requires identification, or whether appropriate design can enable transactions to be undertaken anonymously, or using pseudonyms. Organizations must appreciate that, in many cases, it is entirely feasible for them to protect their interests without knowing their clients' identities.

Government agencies, and some corporations, are seeking to exercise tighter control over individuals using various forms of data surveillance, underpinned by effective identification schemes. Parliaments throughout the world may passively process bills put before them to facilitate such schemes. Alternatively, they may choose to actively seek a balance between the organizational and collective interests on the one hand, and the individual interests on the other. If they adopt this course, then they must proscribe unjustifiably intrusive schemes, promote the use of anonymous and pseudonymous transactions wherever practicable, and, except in carefully justified and regulated cases, deny the multiple uses of identification schemes.