SOFTWARE CONTROL SERVICES (PTY) LTD

475 King's Highway, Lynnwood
P.O.Box 36675, Menlo Park
Pretoria, South Africa
0102

(t) +27 12 348 7301
(f) +27 12 348 1129
(e) techsupport@softconserv.com
www.softconserv.com

Biometrics.

Version 0. 1

Prepared by: Michael Davis- Hannibal

Softcon Software Control Services (Pty) Ltd.

7 March 2017

Revision History

Name	Date	Reason For Changes	Version
MDH	22-Oct-10	Initial document	0.1

Contents

1. General

Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric characteristics can be divided in two main classes:

- Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, which has largely replaced retina, and odour/scent.
- Behavioural are related to the behaviour of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics for this class of biometrics.

Strictly speaking, voice is also a physiological trait because every person has a different vocal tract, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioural.

2. Introduction

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters:

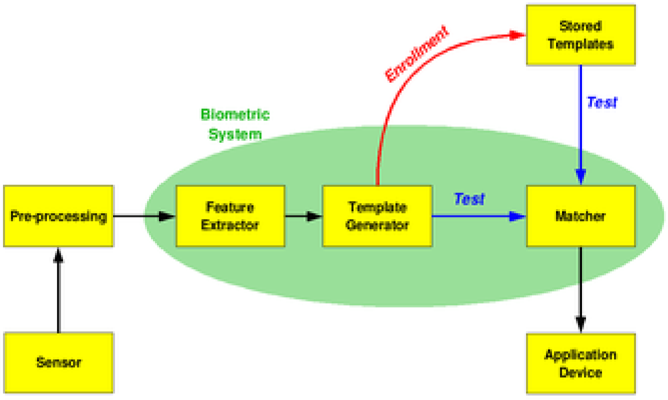

Figure 1: The basic block diagram of a biometric system

- Universality – each person should have the characteristic.
- Uniqueness – is how well the biometric separates individuals from another.
- Permanence – measures how well a biometric resists aging and other variance over time.
- Collectability – ease of acquisition for measurement.
- Performance – accuracy, speed, and robustness of technology used.
- Acceptability – degree of approval of a technology.
- Circumvention – ease of use of a substitute.

A biometric system can operate in the following two modes:

- Verification – A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. Can be done in conjunction with a smart card, username or ID number.
- Identification – A one to many comparison of the captured biometric against a biometric database in attempt to identify an unknown individual. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.

The first time an individual uses a biometric system is called an enrolment. During the enrolment, biometric information from an individual is stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrolment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artefacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrolee.

If enrolment is being performed, the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyse the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area)

3. Performance

The following are used as performance metrics for biometric systems:

- False accept rate or false match rate (FAR or FMR) – the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percentage of invalid inputs which are incorrectly accepted.
- False reject rate or false non-match rate (FRR or FNMR) – the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percentage of valid inputs which are incorrectly rejected.
- Receiver operating characteristic or relative operating characteristic (ROC) – The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- Equal error rate or crossover error rate (EER or CER) – the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.
- Failure to enrol rate (FTE or FER) – the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
- Failure to capture rate (FTC) – Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- Template capacity – the maximum number of sets of data which can be stored in the system.

4. Issues and Concerns

a. Privacy and discrimination

Data obtained during biometric enrolment could be used in ways the enrolled individual does not consent to.

b. Danger to owners of secured items

When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car.

c. Cancellable biometrics

One advantage of passwords over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone’s face is compromised from a database, they cannot cancel or reissue it. Cancellable biometrics is a way in which to incorporate protection and the replacement features into biometrics. It was first proposed by Ratha et al.

Several methods for generating cancellable biometrics have been proposed. The first fingerprint based cancellable biometric system was designed and developed by Tulyakov et al. essentially, cancellable biometrics perform a distortion of the biometric image or features before matching. The variability in the distortion parameters provides the cancellable nature of the scheme. Some of the proposed techniques operate using their own recognition engines, such as Teoh et al. and Savvides et al., whereas other methods, such as Dabbah et al., take the advantage of the advancement of the well-established biometric research for their recognition front-end to conduct recognition. Although this increases the restrictions on the protection system, it makes the cancellable templates more accessible for available biometric technologies.

d. International Trading of Biometric Data

Many countries, including the United States, already trade biometric data. To quote a 2009 testimony made before the US House Appropriations Committee, Subcommittee on Homeland Security on “biometric identification” by Kathleen Kraninger and Robert A Mocny According to article written by S. Magnuson in the National Defence Magazine, the United States Defence Department is under pressure to share biometric data. To quote that article: “ Miller, (a consultant to the Office of Homeland Defence and America’s security affairs) said the United States has bi-lateral agreements to share biometric data with about 25 countries. Every time a foreign leader has visited Washington during the last few years, the State Department has made sure they sign such an agreement. ”

5. Countries applying biometrics

a. United States

The United States government has become a strong advocate of biometrics with the increase in fear of terrorism since September 11, 2001.

The FBI is currently spending $1 billion to create a new biometric database, which will store DNA, fingerprints, and other biometric data. The computers running the database will be contained in an underground facility about the size of a football field.

Both the Department of Homeland Security and DARPA are heavily funding research into facial recognition systems. The Information Processing Technology Office, ran a program known as Human Identification at a Distance which developed technologies that are capable of identifying a person at up to 500 ft. by their facial features.

President Bush issued a presidential directive (NSPD 59, HSPD 24) in 2008 which requires increased capability for sharing and interoperability in "collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals" among the departments and agencies of the executive branch of the U.S. federal government.

Starting in 2005, US passports with facial (image-based) biometric data were scheduled to be produced. Privacy activists in many countries have criticized the technology's use for the potential harm to civil liberties, privacy, and the risk of identity theft. Currently, there is some apprehension in the United States (and the European Union) that the information can be "skimmed" and identify people's citizenship remotely for criminal intent, such as kidnapping.

The US Department of Defence (Dodd) Common Access Card is an ID card issued to all US Service personnel and contractors on US Military sites. This card contains biometric data and digitized photographs. It also has laser-etched photographs and holograms to add security and reduce the risk of falsification. There have been over 10 million of these cards issued.

According to Jim Wayman, director of the National Biometric Test Centre at San Jose State University, Walt Disney World is the nation's largest single commercial application of biometrics. However, the US-VISIT program will very soon surpass Walt Disney World for biometrics deployment.

The United States (US) and European Union (EU) are proposing new methods for border crossing procedures utilizing biometrics. Employing biometrically enabled travel documents will increase security and expedite travel for legitimate travellers.

b. Germany

The biometrics market in Germany will experience enormous growth until 2009. “The market size will increase from approximately 12 million € (2004) to 377 million €” (2009). “The federal government will be a major contributor to this development”. In particular, the biometric procedures of fingerprint and facial recognition can profit from the government project. In May 2005 the German Upper House of Parliament approved the implementation of the ePass, a passport issued to all German citizens which contain biometric technology. The ePass has been in circulation since November 2005, and contains a chip that holds a digital photograph and one fingerprint from each hand, usually of the index fingers, though others may be used if these fingers are missing or have extremely distorted prints. “A third biometric identifier – iris scans – could be added at a later stage”. An increase in the prevalence of biometric technology in Germany is an effort to not only keep citizens safe within German borders but also to comply with the current US deadline for visa-waiver countries to introduce biometric passports. In addition to producing biometric passports for German citizens, the German government has put in place new requirements for visitors to apply for visas within the country. “Only applicants for long-term visas, which allow more than three months' residence, will be affected by the planned biometric registration program. The new work visas will also include fingerprinting, iris scanning, and digital photos”.

Germany is also one of the first countries to implement biometric technology at the Olympic Games to protect German athletes. “The Olympic Games is always a diplomatically tense affair and previous events have been rocked by terrorist attacks - most notably when Germany last held the Games in Munich in 1972 and 11 Israeli athletes were killed”.

Biometric technology was first used at the Olympic Summer Games in Athens, Greece in 2004. “On registering with the scheme, accredited visitors will receive an ID card containing their fingerprint biometrics data that will enable them to access the 'German House'. Accredited visitors will include athletes, coaching staff, team management and members of the media”.

As a protest against the increasing use of biometric data, the influential hacker group Chaos Computer Club published a fingerprint of German Minister of the Interior Wolfgang Chasuble in the March 2008 edition of its magazine Datenschleuder. The magazine also included the fingerprint on a film that readers could use to fool fingerprint readers.

c. Brazil

Since the beginning of the 20th century, Brazilian citizens have had user ID cards. The decision by the Brazilian government to adopt fingerprint-based biometrics was spearheaded by Dr. Felix Pacheco at Rio de Janeiro, at that time capital of the Federative Republic. Dr. Pacheco was a friend of Dr. Juan Vucetich, who invented one of the most complete tenprint classification systems in existence. The Vucetich system was adopted not only in Brazil, but also by most of the other South American countries. The oldest and most traditional ID Institute in Brazil (Instituto de Identificação Félix Pacheco) was integrated at DETRAN (Brazilian equivalent to DMV) into the civil and criminal AFIS system in 1999.

Each state in Brazil is allowed to print its own ID card, but the layout and data are the same for all of them. The ID cards printed in Rio de Janeiro are fully digitized using a 2D bar code with information which can be matched against its owner off-line. The 2D bar code encodes a colour photo, a signature, two fingerprints, and other citizen data. This technology was developed in 2000 in order to enhance the safety of the Brazilian ID cards.

By the end of 2005, the Brazilian government started the development of its new passport. The new documents started to be released by the beginning of 2007, in Brasilia. The new passport included several security features, like Laser perforation, UV hidden symbols, security layer over variable data and etc. Brazilian citizens will have their signature, photo, and 10 rolled fingerprints collected during passport requests. All of the data is planned to be stored in ICAO E-passport standard. This allows for contactless electronic reading of the passport content and Citizens ID verification since fingerprint templates and token facial images will be available for automatic recognition.

d. Iraq

Biometrics are being used extensively in Iraq to catalogue as many Iraqis as possible providing Iraqis with a verifiable identification card, immune to forgery. During account creation, the collected biometrics information is logged into a central database which then allows a user profile to be created. Even if an Iraqi has lost their ID card, their identification can be found and verified by using their unique biometric information. Additional information can also be added to each account record, such as individual personal history.

e. India

India is undertaking an ambitious mega project (the Multipurpose National Identity Card) to provide a unique identification number to each of its 1.25 billion people. The Identification number will be stored in a central database. Consisting of the biometric information of the individual. If implemented, this would be the biggest implementation of the Biometrics in the world. India's Home Minister, P Chidambaram, described the process as "the biggest exercise... since humankind came into existence". The government will then use the information to issue identity cards. Officials in India will spend one year classifying India's population according to demographics indicators.

f. Italy

Italy has standardized protocols in use to police forces. Specialist and University Faculty *Enrico Manfredi d'Angrogna Luserna v. Staufen Rome University Tor Vergata - Siena University.

g. United Kingdom

Fingerprint scanners used in some schools to facilitate the subtraction of funds from an account financed by parents for the payment of school dinners. By using such a system nutritional reports can be produced for parents to survey a child's intake. This has raised questions from liberty groups as taking away the liberty of choice from the youth of society. Other concerns arise from the possibility of data leaking from the providers of school meals to interest groups that provide health services such as the NHS and insurance groups that may end up having a detrimental effect on the ability of individuals to enjoy equality of access to services.

h. Australia

Visitors intending to visit Australia may soon have to submit to biometric authentication as part of the Smartgate system, linking individuals to their visas and passports. Biometric data are already collected from some visa applicants by Immigration. Australia is the first country to introduce a Biometrics Privacy Code, which is established and administered by the Biometrics Institute. The Biometrics Institute Privacy Code Biometrics Institute forms part of Australian privacy legislation. The Code includes privacy standards that are at least equivalent to the Australian National Privacy Principles (NPPs) in the Privacy Act and also incorporates higher standards of privacy protection in relation to certain acts and practices. Only members of the Biometrics Institute are eligible to subscribe to this Code. Biometrics Institute membership, and thus subscription to this Code, is voluntary.

i. Canada

Canada has begun research into the use of biometric technology in the area of border security and immigration (Centre for Security Sciences, Public Security Technical Program, Biometrics Community of Practice). Citizenship and Immigration Canada and the Canada Border Services Agency will probably be the first government institutions to fully implement the technology in Canada.

j. Israel

The Israeli government has passed a bill calling for the creation of a biometric database of all Israeli residents; the database will contain their fingerprints and facial contours. Upon enrolling, a resident would be issued a new form of an identification card containing the biometrics. The law is currently in its trial period, during which enrolment is optional; pending on successful trial, enrolment would be mandatory for all residents.

Opponents of the proposed law, including prominent Israeli scientists and security experts, warned that the existence of such a database could damage both civil liberties and state security, because any leaks could be used by criminals or hostile individuals against Israeli residents.

k. Netherlands

Starting 21 September 2009, all new Dutch passports and ID cards must include the holder's fingerprints. Since 26 August 2006, Dutch passports have included an electronic chip containing the personal details of the holder and a digitised passport photograph. The chip holds following data: your name (first name(s) and surname); the document number; your nationality, date of birth and sex; the expiry date; the country of issue; and your personal ID number (Dutch tax and social security (SoFi) number).

i. Recent requirements for passport photographs

Since 28 August 2006, under EU regulation '2252/2004' all EU member states have been obliged to include a digital image of the holder’s passport photograph.

l. New Zealand

SmartGate was launched by the New Zealand government at Auckland International Airport on Thursday 3 December 2009. It will begin operating in Wellington and Christchurch from next year.

The kiosk and gate system will allow all New Zealand and Australian electronic passport holders over 18 to clear passport control without needing to have their identity checked by a Customs officer.

Deputy comptroller of customs John Secker said SmartGate represented probably the biggest single development in border processing in New Zealand in the past two decades. People will have a choice whether they want to use the system or go through normal passport control.

m. South Africa

Biometrics is becoming more important in the South African and global market. Adelaide Taylor, marcoms manager for ADI in South Africa, says that biometrics is something that will become a global mindset. “With crime occurring all over the world, this is probably the only way to secure your assets and also to protect the people on the premises in future.”

HID’s John Lakin says biometrics have been in extensive use in South African businesses for a number of years and “will remain an important part of an overall security strategy for the foreseeable future. Increasingly they are being used less in isolation and more as part of an integrated security policy. Emerging biometrics, as they prove increasingly reliable, are being adopted in different industries as those businesses continue to search for the perfect solution.”

Rory Webber, national sales manager at Elvey agrees, noting that, from an integration point of view, biometrics are vitally important. “Security solutions are designed with different levels of cover, however with biometrics being able to control both access and time and attendance we have found this to be of great value. Biometrics is not only being used by corporate SA, smaller companies have latched onto the enormous benefits that can be gained by using a biometric system as well.”

Organisations are increasingly switching to biometric solutions for these applications as replacements for legacy card systems, which reaching the end of their lifecycle, say Marius Coetzee, COO of Ideco. “The ROI on a biometric solution far outweighs that of a traditional card-based solution and security is increased as a fingerprint cannot be lost, stolen or forgotten.

“Companies considering a biometric solution must, however, be aware of the risks associated with installing a lesser biometric system, which may seem to be a cost-effective option at the outset, but often ends up costing the clients a lot more when the system proves ineffective and has to be replaced with an accurate and reliable biometric solution. The key to making an informed decision on which biometric system to install lies in understanding how biometric technology works and the experience and track record the supplier has in the field of biometrics.”

6. Biometrics in Popular Culture

- The 2002 film Minority Report features extensive use of casual Iris/Retina scanning techniques for both personal Identification and Point Of Sale transaction purposes. The main character changes his official Identity by having his eyes transplanted, and another character accesses a security system using one of the removed eyes.

- The movie Gattaca portrays a society in which there are two classes of people: those genetically engineered to be superior (termed "Valid") and the inferior natural humans ("Invalid"). People considered "Valid" have greater privileges, and access to areas restricted to such persons is controlled by automated biometric scanners similar in appearance to fingerprint scanners, but which prick the finger and sample DNA from the resulting blood droplet.

- The television program MythBusters attempted to break into a commercial security door equipped with biometric authentication as well as a personal laptop so equipped. While the laptop's system proved more difficult to bypass, the advanced commercial security door with "live" sensing was fooled with a printed scan of a fingerprint after it had been licked.

- In Demolition Man the character Simon Phoenix cuts out a living victim's eye in order to open a locked door which is fitted with iris scanning.

7. References

- en.wikipedia.org
- www.ifsecsa.com