

MULTIMODAL BIOMETRICS FOR VEHICLE ACCESS

Dr. Kashif Qureshi

Department Of Computer Science, tel: +966 (0)535598451, Jazan University,

Jazan, Saudia

srk1521@gmail.com

Abstract:

This paper presents to recognize his/her so many biometrics features will apply to authenticate his/her as follows, the use of multimodal biometrics in order to identify or to verify a person that wants to

start the engine of a car to drive a car or vehicle. First of all, a fingerprint sensor is posted on the car's door, one on the steering wheel, a camera for iris recognition on the car's main mirror, and finally a microphone for voice recognition. There are two possibilities: if the person is identified as the car owner or a known user, then he/she can take control over the car; if

it's an intruder, the car can announce the security service or the police using a complex GPRS (General Packet Radio Service) (GPRS) is a packet oriented Mobile Data Service available to users of Global System for Mobile Communications (GSM) and IS-136 mobile phones. It provides data rates from 56 up to 114 kbps.

GPRS can be used for services such as Wireless Application Protocol (WAP) access, Short Message Service (SMS), Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access. *GPRS data transfer is typically charged per megabyte of throughput, while data communication via traditional circuit switching is billed per minute of connection time, independent of whether the user actually is utilizing the capacity or is in an idle state. GPRS is a best-effort packet switched service, as opposed to circuit switching, where a certain Quality of Service (QoS) is guaranteed during the connection for non-mobile users.*

The multiple access methods used in GSM with GPRS are based on frequency division duplex (FDD) and TDMA. During a session, a user is assigned to one pair of up-link and down-link frequency channels. This is combined with time domain statistical multiplexing, i.e. packet mode communication, which makes it possible for several users to share the same frequency channel. The packets have constant length, corresponding to a GSM time slot. The down-link uses first-come first-served packet scheduling, while the up-link uses a scheme very similar to reservation ALOHA. This means that slotted Aloha (S-ALOHA) is used for reservation inquiries during a contention phase, and then the actual data is transferred using dynamic TDMA with first-come first-served scheduling.) system.

Keywords: multimodal, biometrics, iris, fingerprint, car, access, control, GPRS

Section -1

1. SHORTHISTORY OF AUTOMATIC IDENTIFICATION

Automatic identification and data capture (AIDC) refers to the methods of automatically identifying objects, collecting data about them, and entering that data directly into computer systems (i.e. without human involvement). Technologies typically considered as part of AIDC include bar codes, Radio Frequency Identification (RFID), biometrics, magnetic stripes, Optical Character Recognition (OCR), smart cards, and voice recognition. AIDC is also commonly referred to as "Automatic Identification," "Auto-ID," and "Automatic Data Capture."

AIDC is the process or means of obtaining external data, particularly through analysis of images, sounds or videos. To capture data, a transducer is employed which converts the actual image or a sound into a digital file. The file is then stored and at a later time it can be analyzed by a computer, or compared with other files in a database to verify identity or to provide authorization to enter a secured system. Capturing of data can be done in various ways; the best method depends on application.

AIDC also refers to the methods of recognizing objects, getting information about them and entering that data or feeding it directly into computer systems without any human involvement. Automatic identification and data capture technologies

include barcodes, RFID, bokodes, OCR, magnetic

stripes, smart cards and biometrics (like iris and facial recognition system).

In biometric security systems, capture is the acquisition of or the process of acquiring and identifying characteristics such as finger image, palm image, facial image, iris print or voice print which involves audio data and the rest all involves video data.

Radio frequency identification (RFID) is relatively a new AIDC technology which was first developed in 1980's. The technology acts as a base in automated data collection, identification and analysis systems worldwide. RFID has found its importance in a wide range of markets including livestock identification and Automated Vehicle Identification (AVI) systems because of its capability to track moving objects. These automated wireless AIDC systems are effective in manufacturing environments where barcode labels could not survive.

The most used identification activity in criminology and in common civil applications is the one which has as its aim personal identification. The identification of a person that has committed a crime has been made for a long time by using scientific and mystical elements.

One of the most important innovation in personal recognition and registration belongs to Alphonse Bertillon, police functionary in France, who claimed and demonstrated in 1879 that if many body dimensions - such as waist, width, height, head circumference, the height of right ear, the length of some phalanges and of some bones from the left hand - are measured, then it would be almost impossible to find two individuals with the same characteristics.

It is probably the first "anthropometrical" identification and verification system. This can also be considered as a multimodal biometric system, as it uses many characteristics of the human body. These researches were the first in this important field.

Section -2

2. MODERN BIOMETRIC SYSTEMS

How biometric identification works

Several basic steps are required to make biometric information—our personal physiological features--useful in a contemporary security context. First, our data must be collected as a reference. It does no good to catch a suspected member of a terrorist network and then take her fingerprint.

That fingerprint, or retinal scan, or facial characteristic map must first be on record so that it can be used as a reference when the suspected criminal tries to make it through an airport or cross a country border. Fast computers then use established algorithms to cycle very quickly through their entire collection of references to find a match. If the person crossing the border matches an existing reference at an extremely high threshold, and that reference is for a suspected criminal, then the biometric system has done its job.

Using modern biometrics for identification purposes is not new, nor is it a post-September 11, 2001 phenomenon. Many of the issues raised in the post-attack PATRIOT Act had precursors in a 1996 Counterterrorism bill that would have been signed into law had the ACLU not scuttled it for civil liberties issues.

The technology itself is not newly in use either. As Jerome Rosen pointed out in a 1990 article in *Mechanical Engineering*, a variety of institutions were already using scanners, including the Pentagon; Dade County, Fla. Detention centers; and a newspaper in Little Rock, Arkansas, that used them to have employees punch in and out

Decades ago, when the first biometric technologies were developed, they were much too expensive and complex, being used only in military applications that needed a very high level of security.

The situation changed dramatically because of the progress of informatics technologies and also because of the explosive growth of frauds -it is estimated that every year in the USA, because of the ATM frauds, there are around 500 million dollars lost, 2 billion dollars in the case of cheques, and 1.5 billion dollars from credit cards.

The use of PINs and passwords are not useful anymore for the identification of a person. It is demonstrated, especially in the USA, that if a single document, such as a driving license, is less secure, then all the documents can be obtained by using this counterfeit act.

The following picture shows the percentage of the main fields where the biometrical technologies are used.

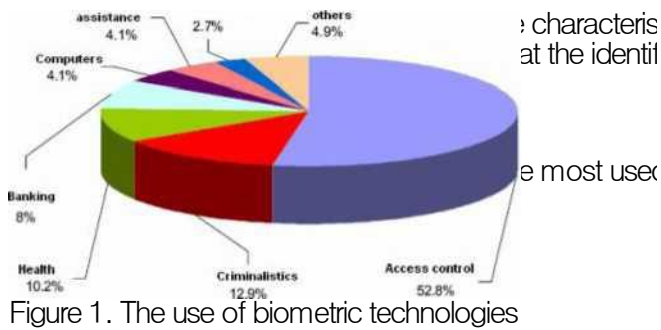


Figure 1. The use of biometric technologies

There are many physiological characteristics traditionally used for identification. The biometric indices can be classified in the following main categories:

- general look/appearance (e.g. height, weight, the color of the skin, hair or eyes, visible characteristic signs, gender, race, facial hair, etc.; all these can be presented in a photo);
- behavior (e.g. general characteristics of the voice, type of character, visible handicaps, features recorded on video tape, etc)
- bio-dynamic elements (e.g. the pressure and the speed of signature, static characteristics of the voice, speed of typing, etc.)
- natural physiological elements (e.g. the dimensions of the skeleton - anthropometrics, healed fractures of the bones, fingerprints and palm-prints, vein structure, iris and retina image, the model of the ear, hand geometry, DNA, etc)
- artificial elements (used especially for the recognition of animals: bracelets, tattooed bar codes, chips implanted under the skin, etc)

Some of these elements, like hair color, weight and height, modify naturally throughout time. The main characteristics of an ideal identification system are presented below:

- universality - every person must be identifiable after the proposed criteria;
- uniqueness - every person must have a single identifier; there should not exist two persons with the same identifier;
- permanence - the identifier must not change during the time, or to be transformed at individual wish;
- necessity - the identifier must contain one or more natural characteristics, at which one person cannot renounce;
- acquisition - the identifier must be easily obtained;
- conservation - the characteristic must be easily stored, in manual or automatic identification systems;
- precision - every identifier must be different enough from another, so that the recognition is made without error.

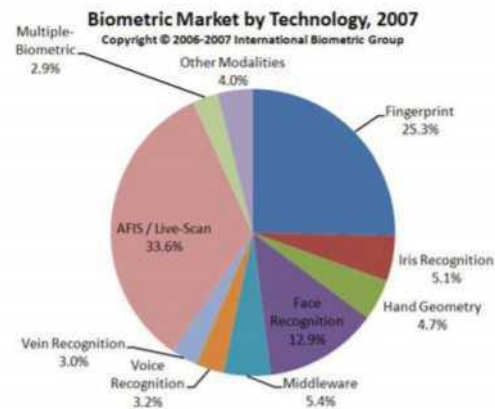


Figure 2. The weight of the biometric technologies

It can be seen from this picture that the main biometric technologies are based on fingerprinting and hand geometry. But, for better accuracy, iris scan can be used, because it's relatively cheap and the results are very promising. The speed of the verification or identification is very small, and the accuracy and uniqueness are at a very high level.

Section -3

3. DESCRIPTION OF THE BIOMETRIC TECHNOLOGIES USED IN THE CAR ACCESS CONTROL

The main biometrics identifiers used in this system are fingerprint, voice, and iris recognition. In the following paragraphs there will be presented the main characteristics of each identifier.

3.1. FINGERPRINT RECOGNITION

Fingerprint.recognition or fingerprint

authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. This article touches on two major classes of algorithms (minutia and pattern) and four sensor designs (optical, ultrasonic, passive capacitance, and active capacitance). The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns.^[1] It is also necessary to know the structure and

properties of human skin in order to successfully employ some of the imaging technologies.

Patterns

The three basic patterns of fingerprint ridges are the arch, loop, and whorl:

- arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
- loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.
- whorl: Ridges form circularly around a central point on the finger.

Scientists have found that family members often share the same general fingerprint patterns, leading to the belief that these patterns are inherited.

This method is probably the most used in personal recognition. It is also one of the first methods of identification and verification. The police use this method to find people who committed different crimes. But this method can be used in civil applications in order to identify the persons. It can be used especially in the access control applications.

The use of fingerprints for identification presents a series of advantages, such as:

- there exists a very significant experience in the use of fingerprints for identification;
- the primary information can hardly be counterfeited, though it is still possible;
- the quantity of information that must be stored is not very high;
- algorithms for processing the fingerprints are very simple, using only 2D mathematical models;
- the precision on of personal identification on is very well;
- it is a completely non-invasive method;
- Identification time is under one second.

The informatics technique used for the recognition of persons is generically called AFIS (Automatic Fingerprint Identification System). The procedure starts with the acquisition of the fingerprint image, then the system automatically marks the zones of interest for the description of the ridges on the image; the points marked on the fingerprint are stored as Cartesian coordinates and are compared with the coordinates stored in the database.

In the following picture it is presented the fingerprint with the points of interest marked and a capacitor sensor for image acquisition.

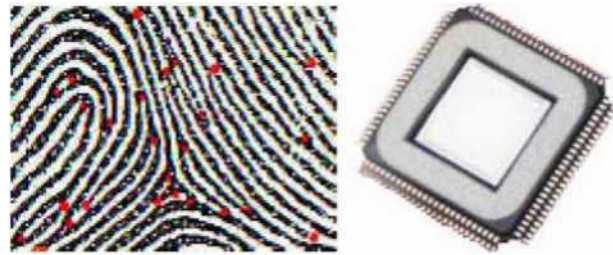


Figure 3. The fingerprint with interest points marked and a sensor for the image acquisition

3.2. IRIS RECOGNITION

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the irides of an individual's eyes, whose complex random patterns are unique and can be seen from some distance.

Not to be confused with another, less prevalent, ocular-based technology, retina scanning, iris recognition uses camera technology with subtle infrared illumination to acquire images of the detail-rich, intricate structures of the iris. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual.^[1] Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per (single-core) CPU, and with infinitesimally small False Match rates.



Many millions of persons in several countries around the world have been enrolled in iris recognition systems, for convenience purposes such as passport-free automated border-crossings, and some national ID systems based on this technology are being deployed. A key advantage of iris recognition, besides its speed of matching and its extreme

resistance to False Matches, is the stability of the iris as an internal, protected, yet externally visible organ of the eye.

In 1987 two Ophthalmology Professors, Leonard Flom, M.D.(NYU) and Aran Safir,M.D.(U.Conn), were issued a first of its kind, broad patent # 4,641,349 entitled "Iris Recognition Technology." Subsequently, John Daugman,PhD (Harvard Computer Science faculty) was then salaried by both ophthalmologists to write the algorithm for their concept based upon an extensive series of high resolution iris photos supplied to him by Dr.Flom from his volunteer private patients. Several years later, Daugman received a method patent for the algorithm and a crudely constructed prototype proved the concept. The three individuals then founded "IridianTechnologies,Inc." and assigned the Flom/Safir patent to that entity that was then capitalized by GE Capital, a branch of "GE"(General Electric) and other investors.

"Iridian" then licensed several corporations to the exclusive Daugman algorithm under the protection of the Flom/Safir broad umbrella patent listed above; thus, preventing other algorithms from competing. Upon expiration of the Flom/Safir patent in 2008 other algorithms were patented and several were found to be superior to Daugman's and are now being funded by U.S. Government agencies.

Mr. John Daugman, from the Cambridge University, developed the main algorithms in iris recognition.

Iris recognition is one of the most accurate methods of personal

identification and verification.

Many companies implemented his method in their software products and created special camera for the acquisition of the image. For example, the Panasonic BM-ET330 is presented below.



Figure 4. Panasonic BM-ET330

The image of the iris is acquired from an iris camera, and then is filtered and recognized in order to obtain a code called IrisCode, which has only 512 bytes. The comparison between two irises is made by calculating the Hamming distance between two codes. This procedure is extremely rapid.

Iris recognition today combines technologies from several fields including, computer vision (CV), pattern recognition, statistical inference, and optics. The goal of the technology is near instant, highly accurate recognition of a person's identity based on a digitally represented image of the scanned eye. The technology is based upon the fact that no two iris patterns are alike (the probability is higher than that of fingerprints). The iris is a protected organ which makes the identification possibilities life long. The iris can therefore serve as a life long password which the person must never remember. Confidence in recognition and identification facilitates exhaustive searches through nation-sized databases.

Iris recognition technology looks at the unique characteristics of the iris, the colored area surrounding the pupil. Most biometrics have 13 to 60 distinct characteristics, the iris is said to have 266 unique spots. Each eye is believed to be unique and remain stable over time and across environments (e.g., weather, climate, occupational differences).

Iris recognition systems use small, high-quality cameras to capture a black and white high-resolution photograph of the iris. Once the image is captured, the iris' elastic connective tissue- called the trabecular meshwork- is analyzed,



processed into an optical "fingerprint," and translated into a digital form. Figure 12 depicts the process of generating an iris biometric. Given the stable physical traits of the iris, this technology is considered to be one of the safest, fastest, and most accurate, noninvasive biometric technologies. This type of biometric scanning works with glasses and contact lenses in place. Therefore, iris scan biometrics may be more useful for higher risk interactions, such as building access. Improvements in ease of use and system integration are expected as new products are brought to market.

The iris is differentiated by several characteristics including ligaments, furrows, ridges, crypts, rings, corona, freckles, and a zigzag collarette.

Iris recognition technologies are now seen in a wide array of identification systems. They are used in passports, aviation security, access security (both physical and electronic), hospitals, and national watch lists. Iris recognition algorithms can be seen in more and more identification systems relating to customs and immigration. Future applications will include, e-commerce, information security (infosec), authorisation, building entry, automobile ignition, forensic applications, computer network access, PINs, and personal passwords.

Advantages of the Iris for Identification

- Highly protected, internal organ of the eye
- Externally visible; patterns imaged from a distance
- Iris patterns possess a high degree of randomness
- variability: 244 degrees-of-freedom
- entropy: 3.2 bits per square-millimeter
- uniqueness: set by combinatorial complexity
- Changing pupil size confirms natural physiology
- Pre-natal morphogenesis (7th month of gestation)
- Limited genetic penetrance of iris patterns
- Patterns apparently stable throughout life
- Encoding and decision-making are tractable
- image analysis and encoding time: 1 second
- decidability index (d-prime): $d' = 7.3$ to 11.4
- search speed: 100,000 Iris Codes per second on 300MHz CPU

Disadvantages of the Iris for Identification

- Small target (1 cm) to acquire from a distance (1 m)
- Moving target...within another...on yet another
- Located behind a curved, wet, reflecting surface
- Obscured by eyelashes, lenses, reflections
- Partially occluded by eyelids, often drooping
- Deforms non-elastically as pupil changes size
- Illumination should not be visible or bright
- Some negative (Orwellian) connotations

3.3. VOICE RECOGNITION

In computer science, **speech recognition** (SR) is the translation of spoken words into text. It is also known as "automatic speech recognition", "ASR", "computer speech recognition", "speech to text", or just "STT". Some SR systems use "training" where an individual speaker reads sections of text into the SR system. These systems analyze the person's specific voice and use it to fine tune the recognition of that person's speech, resulting in more accurate

transcription. Systems that do not use training are called "Speaker Independent" systems. Systems that use training are called "Speaker Dependent" systems.

Speech recognition applications include voice user interfaces such as voice dialing (e.g. "Call home"), call routing (e.g. "I would like to make a collect call"), domestic appliance control, search (e.g. find a podcast where particular words were spoken), simple data entry (e.g., entering a credit card number), preparation of structured documents (e.g. a radiology report), speech-to-text processing (e.g., word processors or emails), and aircraft (usually termed Direct Voice Input).

The term voice recognition^{[1][2][3]} refers to finding the identity of "who" is speaking, rather than what they are saying. Recognizing the speaker can simplify the task of translating speech in systems that have been trained on specific person's voices or it can be used to authenticate or verify the identity of a speaker as part of a security process.

Voice biometrics works by digitizing a profile of a person's speech to produce a stored model voice print, or template. Biometric technology reduces each spoken word to segments composed of several dominant frequencies called formants. Each segment has several tones that can be captured in a digital format. The tones collectively identify the speaker's unique voice print. Voice prints are stored in databases in a manner similar to the storing of fingerprints or other biometric data.

To ensure a good-quality voice sample, a person usually recites some sort of text or pass phrase, which can be either a verbal phrase or a series of numbers. The phrase may be repeated several times before the sample is analyzed and accepted as a template in the database. When a person speaks the assigned pass phrase, certain words are extracted and compared with the stored template for that individual. When a user attempts to gain access to the system, his or her pass phrase is compared with the previously stored voice model. Some voice recognition systems do not rely on a fixed set of enrolled pass phrases to verify a person's identity. Instead, these systems are trained to recognize similarities between the voice patterns of individuals when the persons speak unfamiliar phrases and the stored templates.

A person's speech is subject to change depending on health and emotional state. Matching a voice print requires that the person speak in the normal voice that was used when the template was created at enrollment. If the person suffers from a physical ailment, such as a cold, or is unusually excited or depressed, the voice sample submitted may be different from the template and will not match. Other factors also affect voice recognition results. Background noise and the quality of the input device (the microphone) can create additional challenges for voice recognition systems. If authentication is being attempted remotely over the telephone, the use of a cell phone instead of a landline can affect the accuracy of the

results. Voice recognition systems may be vulnerable to replay attacks: if someone records the authorized user's phrase and replays it, that person may acquire the user's privileges. More sophisticated systems may use liveness testing to determine that a recording is not being used.

Consumer voice recognition systems are typically inexpensive and user-friendly. Most computer systems are equipped to support a microphone used to develop a voice template and later to collect the authentication request. Voice recognition is more often used in an environment in which voice is the only available biometric identifier, such as in telephony and call-center applications. Voice recognition systems have a high user acceptance rate because they are perceived as less intrusive and are one of the easiest biometric systems to use.

Voice verification technology uses the different characteristics of a person's voice to discriminate between speakers. These characteristics are based on both physiological and behavioral components. The physical shape of the vocal tract is the primary physiological component. The vocal tract is made up of the oral and nasal air passages that work with the movement of the mouth, jaw, tongue, pharynx and larynx to articulate and control speech production. "The physical characteristics of these airways impart measurable acoustic patterns on the speech that is produced," as one expert explained.⁹¹ The behavioral component is made up of movement, manner, and pronunciation.

The combination of the unique physiology and behavioral aspects of speaking enable verification of the identity of the person who is speaking. Voice verification technology works by converting a spoken phrase from analog to digital format and extracting the distinctive vocal characteristics, such as pitch, cadence, and tone, to establish a speaker model or voiceprint. A template is then generated and stored for future comparisons.

Voice verification systems can be text dependent, text independent, or a combination of the two. Text dependent systems require a person to speak a predetermined word or phrase. This information, known as a "pass phrase," can be a piece of information such as a name, birth city, favorite color or a sequence of numbers. The pass phrase is then compared to a sample captured during enrollment. Text independent systems recognize a speaker without requiring a predefined pass phrase. It operates on speech inputs of longer duration so that it has a greater opportunity to identify the distinctive vocal characteristics (i.e., pitch, cadence, tone).

Voice verification systems can be used to verify a person's claimed identity or to identify a particular person. It is often used where voice is the only available biometric identifier, such as over the telephone. Voice verification systems may require minimal hardware investment as most personal computers already contain a microphone. The downside to the technology is that, although advances have been made in recognizing the human voice, ambient temperature, stress, disease, medications, and other physical changes can negatively impact automated recognition.

Voice verification systems are different from voice recognition systems although the two are often confused. Voice recognition is used to translate the spoken word into a specific response, while voice verification verifies the vocal characteristics against those associated with the enrolled user. The goal of voice recognition systems is simply to understand the spoken word, not to establish the identity of the speaker. A familiar example of voice recognition systems is that of an automated call center asking a user to "press the number one on his phone keypad or

say the word 'one.'" In this case, the system is not verifying the identity of the person who says the word "one"; it is merely checking that the word "one" was said instead of another option.

Section -4

4. INTRODUCTION TO MULTIMODAL BIOMETRIC SYSTEMS

Multimodal Biometrics are systems that are capable of using more than one physiological or behavioral characteristic for enrollment, verification or *identification*. For biometric identification to be ultra-secure and provide above average accuracy, more than one type must be used as only one form of it may not be accurate enough. One example of this inaccuracy is in the area of fingerprints where at least 10% of people have worn, cut or unrecognizable prints.

Some forms of behavioral *biometric identification* include the following:

- Keystroke or Typing Recognition
- Speaker identification or Recognition

Some forms of *physical* biometric identification include the following:

- Fingerprint
- Iris
- Retina
- Finger Geometry
- Signature/Handwriting
- Voice
- Facial Proportions
- Hand Geometry

Multimodal biometrics will use a combination of the above *recognition* technologies, up to three of them, to compare the *identity* of a person therefore providing the best security available to you. If one of the technologies fails for any reason, your system can still use another one or two of them to provide accurate identification of a person.

The benefits of multimodal biometrics is that by using more than one means of *identification*, your system can retain a high threshold *recognition* setting and your system administrator can decide the level of security that is needed. For a very high security site, you may need to use up to three biometric identifiers and for a lower security site, you may only need one or two of them. This greatly reduces the probability of admitting an imposter.

There is a great need for **multimodal biometrics** as most biometric systems used in real applications are unimodal, which means they rely on only one area of identification. Some examples of these are fingerprints, faces and voices and these systems are quite vulnerable to many problems such as noisy data, non-universality and spoofing. This leads to a

high false acceptance rate and false rejection rate, limited discrimination capability, and lack of permanence.

You can overcome the limitations of unimodal biometric systems by using multimodal biometrics where you use *two or more sources* to validate identity. Multimodal systems are more reliable because you are using many independent biometrics that meet very high performance requirements and they counteract the problems listed above. They also effectively deter spoofing because it is near impossible to spoof *multiple biometric traits* and the system can request the user to present random traits that only a live person can do.

Some of the benefits of using **multimodal biometrics**, and for very secure environments the biometrics could include *fingerprint, iris and voice*, to allow you to safely reset passwords, process payments, and access control to a secure area.

And it can also be used in the following areas:

- Time and attendance keeping
- Border management
- Law enforcement

Multimodal biometrics are driven by various factors such as: risk and viability of spoofing, *universal enrollment* requirements, *accuracy/integrity* requirements, suitability for the environment and transaction time flexibility.

Some of the **multimodal biometrics** target applications are shown below with the potential needed:

Strong Potential:

- Physical access
- Civil ID
- *Criminal ID*

Moderate Potential:

- *Network/PC access*
- Kiosk/ATM

Modest Potential:

- Retail/POS
- *Surveillance*
- ecommerce
- telephony

Now come some of the challenges in designing **multimodal biometrics** systems and the successful pursuit of these challenges will produce great advances to your safety and security in the future. The *sensors* must be consistent in performance under many environmental operations, have embedded privacy functions, protective solutions, enhance public confidence in *biometric technology* and must totally safeguard your personal information.

Biometrics has been adopted in a variety of large-scale identification application – ranging from border control to voter ID issuance. While the technology is conceptually adept, in reality there are numerous challenges associated with enrolling large populations using just single (unimodal) biometrics. These challenges can be overcome by deploying multimodal biometrics systems.

4.1. THE PROBLEMS WITH UNIMODALITY

The shortcoming of unimodal biometrics is that no one technology is suitable for all applications. Therefore, the presence of a multimodal biometric system helps compensate for the following limitations:

- The usage of certain biometrics makes it susceptible to noisy or bad data, such as inability of a scanner to read dirty fingerprints clearly. This can lead to inaccurate matching, as bad data may lead to a false rejection.
- Unimodal biometrics is also prone to inter-class similarities within large population groups. In case of identical twins, a facial recognition camera may not be able to distinguish between the two.
- Some biometric technologies are incompatible with a certain subset of the population. Elderly people and young children may have difficulty enrolling in a fingerprinting system, due to their faded prints or underdeveloped open fingerprint.
- Finally, unimodal biometrics are vulnerable to spoofing, where the data can be imitated or forged.

4.2. DEFINITION OF MULTIMODALITY

Multimodality is the usage of more than one physiological or behavioral characteristic to identify an individual. It involves the fusion of two or more technologies such as fingerprint, facial recognition, iris scanning, hand geometry, signature verification, or speech recognition.

The fusion is done by running the two (or more) biometric inputs against two (or more) different algorithms, to arrive at a decision. This technique is useful in large-scale civil ID applications, where the identity of thousands of people need to be authenticated at a time. To have an additional method of verification as a backup reduces the possibility of inconveniences caused by the malfunctioning of the primary biometric.

4.3. ADVANTAGES OF MULTIMODALITY

It is estimated that approximately 5 percent of any population has unreadable fingerprints, either due to scars or aging or illegible prints. In a civil ID scenario, where millions of people have to be enrolled in the system, the segment of the population who are un-enrollable will face inconveniences. Having multimodal biometric technology can overcome this restriction and ensure lower failure to enroll rate (FTE).

Multimodality can also address the problem of aversion to fingerprinting, found in certain parts of the world. Sometimes people associate fingerprints with criminal activity, and are reluctant to submit prints. By having an additional biometric available, a greater number of people can be enrolled into the

system

Using multiple biometrics solves the problem of inter-class similarity and the resultant high false acceptance rate (FAR). If people with similar hand sizes or similar looking facial features can gain false acceptance, the presence of another biometric such as signature verification can distinguish between the samples.

Another advantage of using multimodality is that it solves the problem of data distortion. If the quality of one of the biometric samples is unacceptable, the other can make up for it. If a fingerprint has been scarred and the scanner rejects the distorted sample, having another modality like facial recognition can prevent high false rejection rates (FRR).

Unimodal Biometrics can be easily spoofed. Placing a high-resolution picture of a fingerprint under the scanner can deceive some systems. However, by using multiple biometrics, even if one modality could be spoofed, the person would still have to be authenticated using the other biometric. Besides, the effort required for forging two or more biometrics is a deterrent to those who wish to do so.

4.4. DISADVANTAGES OF MULTIMODALITY

Some of the disadvantages of multimodal include:

- Interoperability and Standardization: The technology is at its early stages, and there are no universal standards set for storing templates and having all biometrics technologies seamlessly work together.
- Cost: The addition of another biometric technology can drive up the price of the solution. Critics of multimodal systems say it does not offer real value, and that it is just a marketing gimmick geared toward increasing sales.
- Reduced Matching Level: Calculations provided by John Daugman, the originator of the iris algorithm, claim that if a stronger biometric is used in conjunction with a weaker biometric, the result is not necessarily a stronger combined system. The error rate (FAR or FRR) of the weaker biometric can bring down the overall effectiveness of the system.

Major biometrics companies have released products that combine multiple biometrics, mainly for large-scale civil ID usage. Motorola's biometrics unit offers a 'multi-biometric' enrollment and verification solutions with support for fingerprinting, 2D/3D facial recognition, and signature verification. ImageWare Systems also has a middleware product called 'Biometric Engine' that can capture finger, face, and iris data to be used for passport and national ID issuance. Viisage was selected to implement an integrated finger and face biometric system for Iceland's e-passport program. Rather than relying on paper-based images, the facial recognition technology will be used to store a photograph in the passport chip. This will offer higher quality and accuracy levels. The state of Qatar in May 2006, announced the rollout of a national identification project, which will store fingerprint, face, and iris biometric data on a smart card. Similar integration of multiple biometrics with smart card-enabled ID documents is being implemented around the world.

4.5. FUTURE TRENDS

So far, the prominent biometrics combinations have been fingerprint, facial, and iris recognition. It is possible that the patent issue surrounding hand

geometry has made it less accessible for union with multimodal systems. An interesting trend has been the acquisition of companies focusing on a particular biometric technology by companies that make other biometrics. Identity solutions company Viisage, in January 2006, entered into an agreement to merge with Identix, who makes fingerprint scanners. Viisage also acquired the iris recognition company Iridian Technologies, thus becoming competent in facial, fingerprint, and iris biometrics. Similarly, Cross Match Technologies bought out the facial recognition technology company C-VIS, in order to provide multi-modal biometric offerings to their customers. It will be interesting to see if offering a multimodal product triggers the next wave of development within the market, or if it is just a short-term marketing gimmick.

Section -5

5. Conclusion

In this application there are used three main characteristics. The user who wants to use a car must pass all the four tests. First, on the car door there must be a fingerprint reader, then another one on the steering wheel. A microphone records the voice of the user then an integrated chip analyzes these signals. A specialized iris camera takes the iris image and processes it in order to obtain an IrisCode. This code must be compared with the ones stored in a local database. The camera can be placed at the back of the car's main mirror, or it can stay on the board.

After the user passes all this tests, he/she can start the engine of the car. If the user doesn't pass one test, then it can be repeated. After a second attempt, if the test fails, then all collected data is sent by using an integrate GPRS system to the police or/and to an authorized user of the car.

Then, the police can identify the person if his/her characteristics are stored in a database, or can store his fingerprints, voice and iris in a database of criminals.

The main user of the car can introduce other persons in the database by acquiring their images of the fingerprint, voice and iris.

For higher security, both irises can be stored in the database, or more fingers. Of course, many other methods can be combined in order to increase the accuracy of the identification process. Another possibility can be figured out: if the person doesn't possess one biometric identifier, then another one can be used, having in this case a backup biometric identification system. For example, if the person can't talk, then this disability will be stored in the system and only fingerprint and iris verification will work for that person.

REFERENCES:

1. A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans, on Circuits and Systems for Video Technology*, vol. 14, pp. 4-20, Jan 2004.
2. M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," *IEEE Trans, on Patt.*

- Anal. and Mach. Intell., vol. 19, pp. 786–796, July 1997.
3. A. Ross and A. K. Jain, “Information fusion in biometrics,” Pattern Recognition Letters, vol. 24, pp. 2115–2125, Sep 2003.
 4. A. Ross and A. K. Jain, „Multimodal biometrics: *an overview*”, Proc. of *12th* European Signal Processing Conference (EuSIPCO), (Vienna, Austria), pp. 1221–1224, September 2004
 5. *Imran Khan*, „Multimodal Biometrics— Is *Two* Better Than One?”
 6. J.G.Daugman, Combining Multiple Biometrics,
<http://www.cl.cam.ac.uk/~jgd1000/>
 7. www.Wikipedia.com