

A Survey of Unimodal Biometric Methods

Nimalan Solayappan and Shahram Latifi

Department of Electrical engineering, University of Nevada at Las Vegas, USA

Abstract

Apart from making the authentication system reliable, biometric systems reduce the time required for authentication considerably at the airports, borders, and government offices. The paper presents a survey of the unimodal biometric methods that are currently available, and other hybrid forms of biometrics that can be used for security purposes. Some of the latest forms of biometrics that are studied here are the multibiometrics and the combination of the biometrics with other technologies.

Key Words. Finger Print, Iris, Biometric, Security, Vein Recognition

I. INTRODUCTION

As the world is becoming increasingly more insecure, people are looking for new forms of security which are more reliable and less vulnerable against intruders' attacks. One such emerging technology is the field of Biometrics. The term Biometrics is derived from the Greek words bio (life) and metric (to measure). Biometrics is basically a technology that measures and analyzes human physiological and behavioural characteristics for personal identification. The main reason for the acceptance of the biometrics as a tool for security is its universality, distinctiveness, permanence and collectability. Main issues to be considered when implementing a biometric system is performance, acceptability, and circumvention.

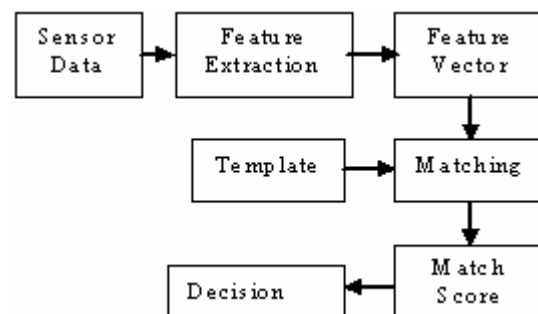
Origin of biometrics dates back to the 14th century in China [3], which was reported by the explorer Joao de Barros. He wrote the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the A biometric system typically consists of a sensor, a feature extraction unit, a matching unit and a decision making unit [2].

young children from one another. In Europe, until the late 1800s, photographic memory was used for the identification. But in the late 1890's Alphonse Bertillon, an anthropologist and police desk clerk in Paris, sought to fix the problem of identifying convicted criminals using biometrics. His method of identification was based on the measurement of adult bones, which doesn't change after the age of 20. This method was eventually named Bertillonage after its founder.

But in the past two decades, there has been an explosion in the biometric industry, where a variety of biometric techniques have been introduced in the market. Some of these techniques deal with recognition based on physical characteristics such as fingerprint, face, iris, retina, hand geometry, vascular pattern, and DNA; others are based on recognition of the behavioral characteristics such as speaker, signature and keystroke.

The paper includes a comprehensive review of biometric systems and the techniques that are used for verification and identification of individuals. The rest of the paper is organized as follows. In section II a typical biometric system and its components are described. So the paper is divided into sections that study the biometric system, biometric techniques, and Performance Comparison.

II. BIOMETRICS SYSTEM



Sensor Unit:

This is where the biometric data is collected. The sensor unit is the most important stage because the accuracy of the entire system ultimately depends on the quality of data that is acquired by the unit. For example in an Iris recognition system, the iris image may be affected by the illumination and by the distance between the camera and the eye.

Feature extraction unit:

This is the stage where the data extracted by the sensor is analyzed, and the features that can be used to identify a person are extracted from the data. Each biometric trait has some features unique to the individual that can be used to identify a person. For example the fingerprint image has features such as whorls, arches, loops, ridges, furrows and minutiae. In iris recognition system, iris features such as rings, furrows and freckles in the colored tissues are used. There are a number of image processing algorithms that are available for feature extraction. The extracted features are represented as a vector, known as the feature vector. Next unit is the Matching unit, where the feature vector is matched with the other feature vectors that are stored in the database.

Matching Unit:

The Matching unit can operate in two modes- verification mode or identification mode. In verification mode, we have to verify if the person is the one who he claims to be. So his biometric trait that was extracted is compared with the one stored in the database. This is basically a one to one matching process. In the identification process the extracted feature is compared to all the features that are stored in the database, which ever comparison gives the best result is taken as the match. So the identification process is a one to many matching process.

The core part of a good matcher is the database that is being used. Much research has been going on in data sharing among different organizations and organizing data in a common database. Biometrics products have to be standardized, so that the databases can be shared among different organizations. Some of the organizations that are working on the standardization of biometrics in the US and in the International front are International Biometric Group (IBG), International Committee for IT Standards, National Institute of Standards and Technology (NIST, standardizing fingerprint searches), International Civil Aviation Organization and Organization for the Advancement of Structured Information Standards (OASIS). [BIOREP]

In a biometric database, the data is stored in the form of templates, representing the biometric measurement of an enrollee, and used by a biometric system for comparison against subsequently submitted biometric samples). So a template is formed using the extracted features from an individual and is compared with the once in the database.

Matching and Decision Unit:

This is the unit that calculates the match between the templates. If the match is above a predefined threshold, then the template is said to be matching. This threshold depends on various factors like the person using the device, level of security that is needed, quality of the biometric trait that has been extracted, etc.

III. TYPES OF BIOMETRICS

a) Fingerprint Recognition:

This recognition process takes an image of the fingerprint either using ink or a digital scanner and records the characteristics such as whorls, arches, loops, patterns of ridges, furrows and minutiae [3],[11]. This information is then stored or processed as an encoded algorithm. There are software programs that can be used to map the minutiae points to their relative placements on the finger and then search for similar minutiae information in the database. To save time during the search process, the image is converted into a character string. Therefore, most of the time the image of the fingerprint is never created, just a string of characters that can be used for comparison.

The finger print reader requires the person to leave his finger on the reader for just a few seconds, during which time it can identify or verify a person. To make sure that a fake finger is not used, these days the fingerprint reader also checks for blood flow or correctly arrayed ridges at the edges of the fingers.

Some of the advantages of this process is that it is a mature technology and user friendly. This method has a very high accuracy, long term stability and supports the option of enrolling multiple fingers to increase the anti-spoofing property. Some of the disadvantages of this method is that the finger print reader might get dirty (because of the contact with the finger), which might affect the quality of the image, or the registered data may vary depending on the skin conditions.

b) Facial Recognition:

This recognition process measures the overall facial structure such as distance between

the eyes, nose, mouth and jaw edges [3],[11]. Using the features, a template is formed and stored in the database. During the verification or identification process the, a person image is obtained using a normal camera or a video camera and a template is formed using the facial features. This template is then compared with the one stored in the database. This system of recognition is currently used only in verification process with much success. To prevent people from faking the system, nowadays the system requires the user to smile, blink or move in a way that is human before verifying.

The advantage of this system is that it is non intrusive; it can be operated at a low cost because the normal security cameras can be used to extract images. In addition, in places such as airports where a high level of security is required, the method can operate covertly; i.e. the image is taken without the knowledge of the individual). Facial recognition has a disadvantage of being highly dependent on the quality of the image obtained, which might be affected by appearance and the environment. This system is generally has low accuracy and might cause problems in case of identical twins. Furthermore, due to its ability to work in a covertly fashion, it has the potential of privacy abuse.

c) Hand Geometry:

This recognition system is a fairly simple procedure but is very accurate [11]. The user places his hand on a metal surface, which has guidance pegs on it, to help the user in aligning his hand properly. The device reads about 90 distinct features of the hand such as the length, width, thickness, surface area of the finger along with the palm size. These features are used to form a template and are stored in the database or can be verified against other template stored into the database.

One of the main advantages of hand geometry technology is that it has one of the smallest templates in the biometrics field, generally under ten bytes. And also has a high user acceptance and it is non intrusive. The disadvantage of this method is that it has low accuracy and it has a relatively large reader. Some people like children, people with arthritis, missing finger, or large hands might find it difficult to enroll. It is used only for the verification process as of now.

d) Iris recognition:

This Technology recognizes individuals by analyzing the features that exist in the colored

tissue surrounding the pupil which includes rings, furrows and freckles.

This is one of the most accurate biometric technologies that are available [4]. In a recent article in Silicon.com, it was stated that in an experiment conducted by the government, which involved facial recognition, iris recognition and fingerprint recognition, it was found that iris recognition was the best among the three for verification process, though its enrollment process was difficult.

The iris image can be obtained using a regular video camera and it can be done from further away than that of a retinal scan. In this technology it is very important that the user cooperates to get a clear image. So the device is such that when the user places his head in front of the device, he would be able to see the reflection of his iris in the device, which shows that a clear image can be obtained. The device may vary the light that is shone into the eye and observe the pupil dilate to make sure that system is not fooled by some fake eye.

The advantage of this system is that it has a good verification rate and resistance to imposter. Iris data is stable with age, and identical for left and right eyes. The disadvantage of this method is that it is highly intrusive; the enrollment process is somewhat difficult because not all people would be comfortable with the system. Much of research on the iris recognition was done by John Daugman, Cambridge University [4].

e) Retinal Recognition:

This method examines the blood vessel patterns of the retina which are supposed to be unique for every individual.

Basically retina consists of sensory tissue with multiple layers, along with photoreceptors like cones and rods which gather the light rays that are sent to it and transforms it into electrical impulses which are in turn converted by the brain into images [11]. The blood vessel in the retina can observe and reflect IR light better than the surrounding tissues in the eye. So the device uses IR light to illuminate the retina and when the IR is reflected back, the retinal scanning device uses it to extract unique features of the retina using different algorithms. The size of the pupil, which determines the amount of light that enters the retina, determines the quality of the image.

The advantages of this technology are that the retina pattern doesn't change over the life time of a person. Compared to other technologies, it has a good verification rate and it

consists of rich unique features. The disadvantage of this method is that there is a public perception that the device might harm the retina, uneasiness of the user when the eye is scanned at a very close distance, the need for the individual to take off glasses on contact lenses, and the requirement of much patience and cooperation by the user.

f) Signature Recognition:

Signature Recognition examines the behavioral aspects in which we sign our name.

This technology is based on the behavioral characteristics like change in timing, pressure, speed, overall size and various directions of strokes during the course of the signing [11]. Even though duplicating signatures seems easy visually, it is not easy to duplicate the behavioral characteristics.

The device consists of a pen (stylus) and specialized writing tablet which is connected to a local computer. The user has to sign on the tablet using the pen. This system collects all the information about the features and forms a template, which is then stored in a database. The user has to sign multiple times to make sure a proper enrollment is done.

The advantage of this technique is that it is a noninvasive tool, widely accepted and difficult to mimic. The disadvantage is that the signature should not be too long or too short because if it is too long then it might contain too many behavioral data and it will be difficult for the system to identify the consistent and unique data points. If the signature is too short, there might not be enough data point for the system to develop a unique template. It should be made sure that the enrollment process is done under the same environmental condition such as standing up, sitting down or resting one's arm. The system is also difficult for the user to get acclimated, which leads to signature inconsistency.

g) Voice Recognition:

Voice originates from the vocal cords. The gap in the vocal cords contracts and expands as we attempt to communicate [10],[11]. So as the gape narrows when we exhale and widens when the breath passes through, unique sounds are created. Vocal tract basically consists of the laryngeal pharynx, oral pharynx, oral cavity, nasal pharynx and the nasal cavity.

In this technique the user is asked to recite a part of text or a list of numbers, using a microphone or any telephone connected to a computer. The computer records the user's voice and converts it from analog to digital format. This format is stored and unique features are extracted from them to form a template. More than one

sample is taken and a statistical profile is made by comparing various samples and determining the various repeating patterns. So the verification is done by comparing the statistical profiles.

The advantage of this method is that the existing telephony infrastructure or simple microphone can be used; it is non intrusive and easy to use. The disadvantages are that the system is affected by background noise; it has very low accuracy and it might be affected by the change of voice due to aging, illness or drinking.

h) Gait Recognition:

Gait recognition is a technology which recognizes individuals by their personal, idiosyncratic manner in which humans walk

Gait recognition is most useful for surveillance because it can be captured without the consent of the person being observed. It is also very difficult to hide and to fake. Some factors that might affect gait are stimulants like alcohol and drugs which makes a person unbalanced, physical changes due to pregnancy, accident, after weight gain or weight loss, a person's mood, and the clothes worn by them.

Gait recognition can be done using normal surveillance cameras. Some of the advantages are that it can be done from a distance and low cost surveillance cameras can be used. The disadvantages are that it can be easily faked and be affected by the background, clothes and feelings of the person.

i) Key stroke Recognition:

Keystroke Recognition is based on the fact that the manner in which we type our computer keyboard varies from person to person.

This technique consists of a keypad or a key board that is connected to a computer. The user is asked to type a set words at different periods of time [11]. Certain conditions need to be met such as one has to type without corrections; in case of a mistype one he has to start again, etc. Some the feature that are extracted are- the way a person types, the cumulative typing speed, time that elapses between consecutive strokes, time that each key is held down, frequency of the individual in using other keys on the keyboard, such as the number pad or function keys and the sequence that is utilized when typing a capital letter for example, and whether the individual release the shift key or the letter key first. Using these features a template is created forming a statistical profile of the individual's behavioral characteristics.

The advantages of these methods is that they are purely software based, do not require additional hardware, can be integrated with other

biometrics, and minimal training is required. Another advantage is that if the template is created for a specific word and the template is tampered, then the word can be changed and a new template can be formed. The disadvantage is that the method does not ease the burden of remembering the passwords. In addition the technology is in its very early stage and has not been tested on a wide scale.

j) Hand Vascular Pattern Recognition:

The technology verifies or recognizes human users by utilizing a state-of-the-art recognition algorithm based on unique veins and capillaries found on the back of the human hand.

Vein pattern recognition is based on the concept that during infrared imaging, the hotter an image, the lighter it looks; and the colder an object, the darker it appears [6]. So when a hand is scanned by an infrared reader, the vein pattern appears darker than its surroundings. The pattern for each and every person is different. If the image is saved as a template for a person, it can then be used for verification or identification purposes.

The advantages are that the method has a high accuracy; it is not affected by the harsh environment such as construction site, military bases, manufacturing factories, etc. It is also very convenient for the user because minimum knowledge of the system is required. Infrared absorption patterns are easily compared via optical and DSP techniques providing a large, robust, and stable basis for the matching unit. This generally requires a low resolution IR.

k) DNA (Deoxyribo Nucleic Acid):

This technology uses the DNA pattern of a person to identify them [7]. DNA was discovered in 1868. Since then people have learned how to use and manipulate DNA for various applications. DNA molecules are made of a long string of chemical building blocks called "nucleotides". The sources of DNA are Blood, Semen, Tissues, Chemically treated Tissues, Hair Roots, Saliva, Urine, etc.

DNA technology has been used extensively in Forensic field and to establish paternity and other family relationships. Apart from this, it is also used to match organ donors with recipients in transplant programs; determine pedigree for seed, and improve crops. This technology has also been used to rapidly detect and identify new outbreaks of deadly diseases such as SARS.

Advantages of DNA are that they can be found in almost every cell in the body, and the technique has an extremely high compared to other biometrics. The disadvantages are that the DNA samples are prone to degradation and contaminations from external sources, and the control and storage of DNA would have to deal with a lot of privacy acts.

IV.PERFORMANCE COMPARISON

Not all biometrics mentioned above give the same level of performance. The performance of each biometric also depends on the kind of application. So it is very important to know how the biometrics perform comparatively. In the following, we examine some comparison results.

a) Most constant Biometric feature over time:

Some biometric features may change over time due to various reasons such as

- Growth
- Aging
- Dirt and grime
- Injury and subsequent regeneration etc.

<i>Biometric Trait</i>	<i>Permanence over time</i>
Fingerprint (Minutia)	oooooooo
Signature (dynamic)	oooo
Facial structure	oooooo
Iris pattern	oooooooooooo
Retina	oooooooooooo
Hand geometry	oooooooo
Finger geometry	oooooooo
Vein structure of the back of the hand	oooooooo
Ear form	oooooooo
Voice (Tone)	ooo
DNA	oooooooooooo
Odor	oooooo
Keyboard strokes	oooo
Comparison: Password	ooooo

The table above shows how constant each biometric trait is over a period of time. The more circles in the second column, the more constant is the respective trait is over a period of time. It is seen from the table that the Iris recognition and DNA are the most constant over time. Voice trait is the least constant biometric.

b) Comparison based on other aspects:

The charts below were presented by National Center for State Courts (NCSC) [3]

Biometric	Verify	ID	Accuracy
Fingerprint	Yes	Yes	High

Facial Recognition	Yes	No	Medium
Hand Geometry	Yes	No	Medium
Speaker Recognition	Yes	No	Low
Iris Scan	Yes	Yes	High
Retinal Scan	Yes	Yes	High
Signature Recognition	Yes	No	Low
Keystroke Recognition	Yes	No	Very Low
DNA	Yes	Yes	High

Signature Recognition	Medium	Medium	Non
Keystroke Recognition	Low	High	Non
DNA	High	Low	Extremely

Biometric	Reliability	Error Rate	Errors
Fingerprint	High	1 in 500+	dryness, age, dirt
Facial Recognition	Medium	no data	lighting, age, glasses, hair
Hand Geometry	Medium	1 in 500	hand injury, age
Speaker Recognition	Low	1 in 50	noise, weather, colds
Iris Scan	High	1 in 131,000	poor lighting
Retinal Scan	High	1 in 10,000,000	glasses
Signature Recognition	Low	1 in 50	changing signature
Keystroke Recognition	Low	no data	hand injury, tiredness
DNA	High	no data	none

Biometric	Ease of Use	Low Cost	Hardware	Standards
Fingerprint	High	Yes	Special, Cheap	Yes
Facial Recognition	Medium	Yes	Common, Cheap	?
Hand Geometry	High	No	Special, mid-price	?
Speaker Recognition	High	Yes	Common, Cheap	?
Iris Scan	Medium	No	Special, expensive	?
Retinal Scan	Low	No	Special, expensive	?
Signature Recognition	High	Yes	Special, mid-price	?
Keystroke Recognition	High	Yes	Common, Cheap	?
DNA	Low	No	Special, expensive	Yes

Biometric	Long Term Stability	User Acceptance	Intrusive
Fingerprint	High	Medium	Somewhat
Facial Recognition	Medium	Medium	Non
Hand Geometry	Medium	Medium	Non
Speaker Recognition	Medium	High	Non
Iris Scan	High	Medium	Non
Retinal Scan	High	Medium	Very

Aspect description of the chart

Verify: Whether or not the Biometric is capable of verification.

ID: Whether or not the Biometric is capable of identification.

Accuracy: How well the Biometric is able to tell individuals apart. This is partially determined by the amount of information gathered as well as the number of possible different data results.

Reliability: How dependable the Biometric is for recognition purposes.

Error Rate: This is calculated as the crossing point between graphs of false positives and false negatives created using the Biometric.

Errors: Typical causes of errors for this Biometric.

Long-term Stability: How well this Biometric continues to work without data updates over long periods of time.

User Acceptance: How willing the public is to use this Biometric.

Intrusiveness: How much the Biometric is considered to invade one's privacy or require interaction by the user?

Ease of Use: How easy this Biometric is for both the user and the personnel involved.

Low Cost: Whether or not there is a low-cost option for this Biometric to be used.

Hardware: Type and cost of hardware required to use this Biometric.

Standards: Whether or not standards exist for this Biometric.

c) Template Size:

Another important aspect that has to be considered is the template size of each biometrics [10]. This is due to the fact that the biometric traits are stored as database and in recent times they are used in smartcards.

Biometric	Approx Template Size
Voice	70k - 80k
Face	84 bytes - 2k
Signature	500 bytes - 1000 bytes
Fingerprint	256 bytes - 1.2k
Hand Geometry	9 bytes
Iris	256 bytes - 512 bytes
Retina	96 bytes

VII.CONCLUSION

We conclude that Biometrics plays a crucial role in the security system of the future. It is too early to predict how bigger role it would play because a number of the biometric systems are still in the testing stages. It can also be said that a unimodal biometric is not enough and would never fully serve the purpose that we are looking for. So it is best to look at other forms of biometrics such as Multibiometrics and combination of biometrics and technologies such as RFID and Smartcards.

Reference:

- 1) "Multibiometric Authentication", Uwe M. Bubeck, San Diego State University
- 2) "Information Fusion in Biometrics", Arun Ross, Anil Jain, Department of CS & Eng., Michigan State University
- 3) "History, Summary of Different Biometric Traits, Comparison Chart", *National Center for State Courts (NCSC)*.
- 4) "How Iris recognition works?", John Dougman, University of Cambridge
- 5) "Ear Biometric", Hanna-Kaisa Lammi, Lappeenranta University of Technology, Department of Technology, Finland

- 6) "Vein Biometric Home Page", Joesph Rice, ntlworld.com
- 7) "How DNA Evidence Works", Ann Meeker-O'Connell,<http://www.howstuffworks.com/dna-evidence.htm/printable>
- 8) "Types of Biometrics", Biometric Institute, <http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=30>
- 9) "Multi-Modal Versus Uni-Modal Performance in Biometrics", Kevin W.Bowyer, <http://www.biometrics.org/bc2004>
- 10) "CSCI E-170: Computer Security, Privacy and Usability", http://www.simson.net/csci_e-170/handouts
- 11) Summary of various Biometric traits, HTG Advance Systems <http://www.htgadvancesystems.com/Advance/marketing/>
- 12) General RFID Information, RFID Journal, <http://www.rfidjournal.com/faq>