ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

"A survey of biometrics: features, components, examples and applications"

Ruaa Adeeb Abdulmunem Al-falluji

University of Babylon, Babylon, Iraq

Abstract: Biometric is newest technology in the security field. It uses the inherent characteristic to authenticate persons. This in turn will enhance the reliability of the security systems compared to the traditional based authentication systems such as password or code and solve many of the problems that appeared in the traditional based systems. This leads to using biometrics systems widely in many applications . Many features in the human's body can be used as biometrics if they meet specific requirements .Each one of these biometrics have strength and weakness points. This paper will discuss the commonly used biometrics.

Keywords: Biometrics,Authentication,Verification,Identificatin,Feature Extraction.

I. INTRODUCTION

Because of the numerous problems of the traditional-based security technologies, there is a demand for producing suitable security barriers which are reliable and low-cost especially when our society gets more and more computer dependent. Biometrics is seen as the way forward as it provides the good level of security by recognizing/verifying the people based on their personal characteristics.

There are many biometrics systems being developed using fingerprints, voiceprints, facial characteristics, eye features, hand geometry….etc.These computers based security systems are used at various fields like commercial, civilian and government offices and many other fields.

This research illustrates what "Biometrics" means and explains the characteristics of any human biometric. The general components of biometric systems and their work phases will be shown. Then it discusses the most common types of biometrics with their strengths and weaknesses and gives a comparison between common biometrics. Finally, we will illustrate the applications of biometrics systems.

II. BIOMETRICS

The term “biometrics” can be broken down into two components: bio and metrics. The translation for “bio” is living organism, and for “metrics” is measurement. So biometrics is “the measurement of living organisms” [1, 2].

We can more specifically define biometrics as "the science and technology of measuring and analyzing human physiological and behavioral characteristics such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for security purposes" [1].

The power of the biometric systems is that they provide a nontransferable means of identifying people not just cards or badges. These" nontransferable" means cannot be given or lent to another individual so nobody can get around the system - they personally have to go through the control point.

A. Desirable Features of Biometrics

Any human physiological or behavioral trait can serve as a biometric characteristic as long as it possesses the following features [3,4,5]:

1. **Universality,** which indicates that everybody should have this characteristic.
2. **Uniqueness,** which means that no two people should be the same in terms of the characteristic.
3. **Permanence,** which indicates that the characteristic should be invariant with time.
4. **Collectability,** which means that the characteristic should be collectible by anyone on any occasion, i.e. can be measured quantitatively.
5. **Performance,** which refers to the achievable identification accuracy, the resource requirements to achieve acceptable identification accuracy, and the working or environmental factors that affect the identification accuracy.
6. **Acceptability,** which indicates to what extent people, is willing to accept the biometrics system.
7. **Circumvention Resistance**, which refers to how easy it is to fool the system by fraudulent techniques.
8. **Cost Effectiveness,** which indicates that measuring and storing the characteristic, is not being unduly costly.
9. **Simplicity,** which means that recording and transmission should be easy and not error-prone.

B.Components of Biometric Systems

Typically, simple biometric system consists of the following main components [1, 6, 7, 8]:

1. **Sensor Unit:** This is where the biometric data are collected. The sensor unit is the most important stage because the accuracy of the entire system ultimately depends on the quality of data that are acquired by this unit. A recorder is a type of the sensors that can be used. Many conditions should be taking into account to capture standard biometric data such as the distance between sensor and human.

DOI 10.17148/IJARCCE.2015.4948

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

2. **Preprocessing Unit**: In this unit, many preprocessing steps are implemented on the images acquired in the previous unit like filtering and enhancing techniques to get rid of any noise, undesirable information and keep just the required regions. These steps will facilitate the work that must be done in the next units and make it quicker.

3. **Features Extraction Unit:** Each biometric trait has unique characteristics that can be measured to identify or verify a person. In this stage the collected data are analyzed and these biometric features are extracted. For example, if hand geometry would be used as a biometric trait then the used features would include width of the palm, thickness of the palm, length of fingers… etc. There are many computer vision algorithms employed for features extraction. According to the selected biometric and its application the suitable features extraction technique can be chosen [8, 9]. The gained result after applying these algorithms is called a template which contains all the extracted features.

4. **Matching Unit:** Within this unit comparison between the newly acquired data and the previously stored data occur. Matching may be either one to one if the system will be used for verification or one to many if it will be used for identification. Different types of matching techniques can be used such as statistical distance based classifiers, shape matching techniques and so on. According to our system and its use, we can choose the most suitable matching technique. The decision is made based on the results of the matching unit, the user's identity is either established (in identification) or a claimed identity is accepted or rejected (in verification). Fig. 1 shows the components and the logical flow of a typical biometric system.

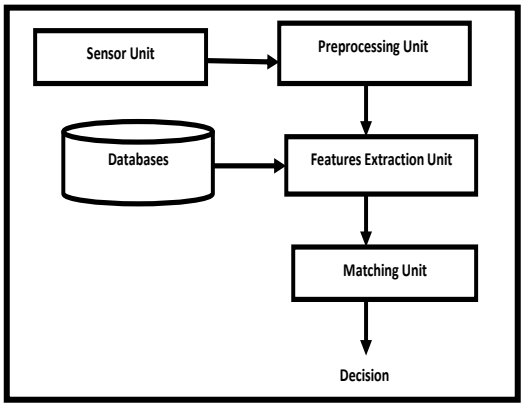

Fig. 1. Typical biometric system components

C.The Work Phases of Biometric Systems

In general biometric systems work in two phase [6, 10,11]:

- **Enrollment Phase:** In this phase the biometric data are acquired from the user either by scanning or by taking photographs. The gathered data are then processed to create a template. A template is a compact version of the original representation where certain features are measured. Afterwards, the template is stored in a database where it is labeled with user identity (e.g. name, identification number) to facilitate authentication. It can also be stored on an external device such as a smart card.
- **Authentication phase:** The data of the new users will be acquired to authenticate them. The biometric system can be either for verification or identification purpose. In **verification mode,** the user claims an identity and the comparison process is limited to checking if the user claim is true or not. The user is verified if the stored template corresponding to this identity is the same as the newly acquired data (i.e. one to one matching). While in **identification mode** no claim of identity is necessary. The system searches its database to find if stored templates match the newly biometric data acquired from the user (i.e. one to many matching). Fig. 2 shows in three diagram the enrollment, verification, and identification phases respectively.

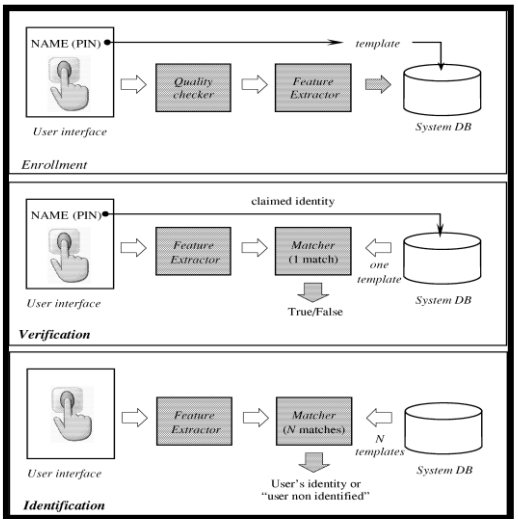

Fig. 2.Block diagrams of enrollment, verification, and identification tasks of the biometric system [11]

D.Biometric Systems Examples

Here, a summary of the existing and emerging biometric technologies will be given taking into account the strengths and weaknesses of each biometric characteristic.

Fingerprint

Among all the biometric techniques, fingerprint is the oldest one which has been successfully used in numerous applications. In a fingerprint recognition system an electronic device , sensor, used to capture a digital image of the fingerprint pattern. Many types of sensors may be used such as optical, ultrasonic and capacitance sensors. The captured image is called a live scan. This live scan is digitally processed to create a biometric template. A fingerprint template is a collection of extracted features such as whorls, arches, loops, patterns of ridges, furrows and minutiae which are stored and used for matching.

Fig. 3 shows a sample of a binary fingerprint, the important thing which must be noticed here is that the actual fingerprint image is not recorded just some data points, called minutiae, will be recorded. During the matching process the relationships between the new and recorded data points will be measured.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Fig. 3. Fingerprint Sample

Merits:
- It is a user friendly.
- It assures high accuracy.
- Its templates are of long term stability.

Demerits:
- Contact readers may affect the quality of the image.
- Variations of the registered data may occur due to the skin conditions [3].

Face

The persons' images will be captured by using either a normal or a video camera. Then many features such as shape of the eyes, eyebrows, nose, mouth, chin, lips and jaw edges in addition to the relationships between these attributes are measured. After that templates are created and stored in database to use them in comparisons for verification or identification purposes.

Nowadays, to prevent counterfeit many facial expressions are taken into account during capturing images such as sadness, happiness, anger, amazement expressions and so forth. Fig. 4 shows the acquired facial images with expressions [12].

Fig. 4.Six different facial expression images for the same person

Merits:
- It is cheap because of using low cost normal security cameras for image acquisition.
- It can operate covertly; this means that the image can be captured without the knowledge of individuals so it is very preferable when high level security is required.

Demerits:
- It is highly dependent on the quality of the acquired images which themselves may be effected by many factors such as environment.
- The difficulty of matching step in these systems because of using high amount of facial elements.
- Many problems appear in the case of identical twins.

Hand Geometry

Hand geometry is a biometric trait that verifies or recognizes persons based on the geometric structure of their hands. In the hand geometry based systems, the user places his/her hand on a metal surface according to guide marks in order to help user in aligning his/her hand properly. Many measurements are taken into account in these systems such as hand shape, width of the fingers at various locations, width of the palm, thickness of the palm, length of the fingers... etc. Fig. 5 shows the possible features that might be collected to create the template that is stored in database to be used later in authentication process [13].

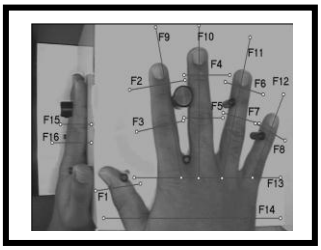

Fig. 5: sixteen axes along which features values are computed from hand

Merits:
- It is a very simple and easy to use method.
- It has a high user acceptance.
- The templates of these systems are the smallest in the biometrics field, although the high amounts of the features which are included within them.

Demerits:
- It has a large reader compared to other biometrics readers.
- The difficulty of enrollment process in some people like children, people with arthritis and missing fingers.
- It has a low accuracy.
- Until now, it is used for only verification process [1, 7, 14].

Iris

Iris recognition is among the most known biometric technologies in the market today. This technology based on the features that exist in the colored annular region of the human eye as shown in Fig. 6.

The iris image can be captured using a regular video camera, and the features of iris are analyzed to create a template which is used later to make decisions about giving authentications or not.

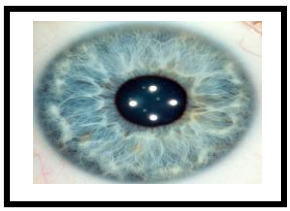

Fig. 6. Example of an iris image

Merits:
- It is the most accurate biometric trait.
- Its patterns apparently stable throughout life.
- Its high resistance to imposters.

Demerits:
- The difficulty of the enrollment process due to the uncomfortability of most of the people [1, 2, 7, 15, 16].

DOI 10.17148/IJARCCE.2015.4948

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Retina

The patterns of retinal blood vessels were found to be unique for every individual; even for the eyes of the identical twins. This led to the evolution of the retinal recognition/verification research field. Infrared retinal scanning device is used to capture retinal images which are analyzed to extract features. After that, the extracted features are combined to create the retina template.

Templates are stored in databases to be used later for individuals' authentication. An example of a retina image can be shown in Fig. 7.

Fig. 7: Retina image

Merits:

- It has a very high accuracy.
- There is no way to counterfeit the retina.
- The eye from a dead person would deteriorate too fast to be useful, so there is no need to additional precautions to be taken with retinal scans to ensure that the user is a living human being or not.

Demerits:

- The difficulty of enrollment process due to the public perception that scanner device is harmful to the eye.
- Its reader is very expensive.
- It can be affected by the diseases such as glaucoma, diabetes and high blood pressure.
- It is highly affected by glasses and lenses [1,17].

DNA (Deoxyribonucleic Acid)

This technology uses the DNA patterns of persons that can be extracted from blood, hair, and skin…..etc as a biometric characteristic to identify or verify them.

Merits:

- It has a high availability, because DNA can be found in almost every cell in the human body.
- It is a high accuracy technology.

Demerits:

- The similarity problem of DNA patterns in identical twins.
- DNA samples are prone to degradation and contaminations from external sources.
- The control and storage of DNA patterns requires special conditions [1, 20].

Signature

This technology is based on the behavioral characteristics in the person's signature like pen pressure, speed, overall size of signature….etc.The used device in these systems consists of a pen and a writing tablet connected to a computer. The user has to sign on the tablet using the pen. All features will be measured to create a template, which is then stored in a database to be used in making the decision. A sample of signature can be shown in Fig. 8.

Fig. 8. Example of scanned signature

Merits:

- It has a high social acceptability.
- The professional forgers are capable of reproducing signatures but the behavioral characteristics of the signatures could not be duplicated.

Demerits:

- The signature's length should not be too long or too short because of the difficulty of analyzing features or dis-availability of the enough information, respectively.
- The enrollment process must be done under the same environmental conditions such as standing up, sitting down...etc.
- The difficulty of users' acclimatization with the system [1, 2, 18].

Vein Patterns

Vein patterns recognition/verification is indeed the newest among the biometric techniques, which makes use of vein patterns that are found in four different regions of human's body as a biometric measure such as the veins in the back of the hand, the veins in the wrist, the veins in the palm of the hand, and the veins in the fingers.

The vein patterns recognition process begins with capturing vein patterns images either by near infrared (NIR) or by thermal (far infrared (FIR)) imagining. Fig.9 shows vein patterns images for the four regions that are previously mentioned.

When the target is placed on a scanner an infrared light passes through the tissue and the rays are absorbed by the red blood cells (Hemoglobin). So, the veins will appear as black lines while the rest of the region structure appears as white. After that the features are extracted from the captured images and the templates will be stored in the database which will be used then for matching to make decisions.

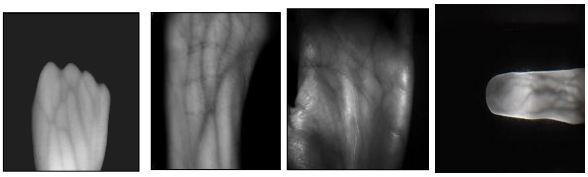

Fig. 9: Samples for veins patterns at(from the left) a) the back of the hand b) the wrist, c) the palm of the hand, d) the finger

Merits:

- It is fast, easy to use technology (only minimum knowledge with the system is required).
- Live body identification, a vein image just can be taken at live body, thus the vein image at non-live hand cannot be read and taken, accordingly no identification and authentication can be made. So no falsification can be made.

DOI 10.17148/IJARCCE.2015.4948

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

- Its difficulty to forginning by imposters because the blood vessels are hidden within the body.
- The human vascular structure is unique for each individual.
- Identical twins have different and distinct IR absorption patterns.
- Vein patterns are stable and never change over the life time only by their size.
- Approximately it is a low cost biometric technology.
- It has a high accuracy.
- Low resolution IR is required.

Demerits:

- There are many factors can effects on the quality of the captured image such as unevenly distribution of heat.
- The hair which may be found on the surface of the back of the hand acts as a source of noise because of the existence of the keratin that absorbs most of the incident IR radiation which makes it appears dark and this affects the veins appearance.
- Thick fat layer which may be found in some people can partially prevents the appearance of veins in thermograms.
- Little number of algorithms fit for vein recognition [1, 3, ,8,19, 20, 21].

E. Comparison between the Commonly Used Biometrics

As we mentioned above that each biometric technology has its strengths and limitations. Table 1 gives us a brief comparison between the most commonly used biometric techniques [4, 11].

TABLE 1: COMPARISON BETWEEN COMMONLY USED BIOMETRICS

Biometric Characteristic	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention Resistance	Cost Effectiveness
Finger print	M	H	H	M	H	M	M	M
Face	H	M	M	H	M	H	M	M
Hand-Geometry	M	M	M	H	M	M	M	M
Iris	H	H	H	M	H	L	H	L
Retina	H	H	H	L	M	M	M	L
DNA	H	H	H	L	L	L	M	L
Signature	L	L	L	M	L	H	M	M
Vein Patterns	M	H	H	M	M	M	H	M

(Where H=High, M=Medium, L=Low)

One of the notices that we can see from the above table is that just the resistance of vein patterns and iris technologies to the circumvention is high and thus in turn show the reliability of these techniques.

Also there is a very important issue must be noticed that no biometric is expected to effectively meet all the needs of all applications i.e. the technology that meets the requirements of a specific application may not achieve the requirements of other applications. This means that according to our application requirements we can select the suitable biometric technology [3, 4, 11, 22, 23].

F. Applications of Biometric Systems

In the last few years, the area of applications of biometrics has increased and it's expected that in the near future, we will use biometrics on many aspects in our daily life.

Depending on where the biometrics is deployed, the applications can be categorized in the following five main groups [3, 11, 24]:

- **Forensic Applications :** Such as criminal investigation ,terrorist identification, parenthood determination, missing children, corpse identification….etc.
- **Government Applications :** Such as national identification cards, driver's licenses, military programs.
- **Commercial Applications :**Such as account access, online banking, time and attendance monitoring, physical access.
- **Health-Care Applications :** Such as patient identification, patients' access to their personal information.
- **Traveling and Immigration Applications:** Such as passports, border crossing.

III. CONCLUSION

Each biometric feature may have many points of strength and weakness. We can deduce that no biometric technique is foolproof. Therefore we can select the suitable technique according to our application; in another meaning we cannot find a system that is suitable for all applications until now.

IV. FEATURE WORK

One of the solutions to strengthen the security systems is to combine two or more of the biometric traits. Another solution is to combine a traditional security technology like password with a biometric trait , this may also make the system more reliable and difficult to be attacked by imposters.

REFERENCES

[1] Latifi S, Solayappan N , "A Survey of Unimodal Biometric Methods", International Conference on Security & Management, Las Vegas, USA,2006.
[2] Halim Sayoud, "Biometrics: An Overview on New Technologies and Ethic Problems", International Journal of Technoethics, Vol. 2, No.1, p.p. 19-34, 2011.
[3] M. K. Shahin, "Hand Vein based Biometric Verification System", Master Thesis, Cairo University, Faculty of Engineering, Systems and Biomedical Dept., 2005.
[4] Anil Jain, Ruud Bolle, Sharath Pankanti, "Biometrics Personal Identification in Networked Society", First Edition, 1999.
[5] Roger Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues", Journal of Information Technology & People ,Vol.7,No.4 , 1994, p.p. 6-37.
[6] Bohm Igor, Tester Florian, "Biometric Systems: Report", Department of Telecooperation, University of Linz, Austria, 2006.
[7] Sulochana Sonkamble, Dr. Ravindra Thool, Balwant Sonkamble, "Survey of Biometric Recognition Systems and Their Applications", Journal of Theoretical and Applied Information Technology, Vol. 11, No. 1, 2010.

DOI 10.17148/IJARCCE.2015.4948

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

[8] Sanya-Isijola, Ademuyiwa,"Vein Pattern Recognition Biometric Systems", University of East London,2010.
[9] Jeng-Shyang Pan ,Shu-Chuan Chu, Pei-Wei Tsai, Hao Luo, Fa-Xin Yu , "A survey of Vein Recognition Techniques", Information Technology Journal ,Vol. 9, No. 6, p.p. 1142-1149, 2010.
[10] bsigroup-website.[online].Available: http://shop.bsigroup.com/en/Browse-By-Subject/Biometrics/How-do-biometric-systems-work/
[11] Anil K. Jain, Arun Ross, Salil Prabhakar , "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.
[12] Aliaa A. A. Youssif, Wesam A. A. Asker ,"Automatic Facial Expression Recognition System Based on Geometric and Appearance Features", Computer and Information Science Journal, Vol. 4, No. 2, March 2011.
[13] Anil K. Jain, Arun Ross , Sharath Pankanti " A Prototype Hand Geometry-based Verication System", Proceedings of Second International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), Washington D.C., p.p. 166-171, March 22-24, 1999.
[14] Nader Abd El-Rahman Mohamed Shaaban, "A Prototype of Automatic Hand Geometry Verification System ," MasterThesis, Cairo University, Faculty of Engineering, Systems and Biomedical Dept., 2002.
[15] Human recognition systems website**.** [online] .Available: http://www.hrsid.com/technology
[16] John Daugman, "How Iris Recognition Works", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, p.p. 21 – 30, 2004.
[17] Biometrics and Authentication in Elearning wiki.[online] .Available: http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies
[18] Adams Wai Kin Kong,"Palmprint Identification Based on Generalization of IrisCode", Ph.D. Thesis,University of Waterloo, Faculty of Engineering, Electrical and Computer Dept., 2007.
[19] Annemarie Nadort, "The Hand Vein Pattern Used as a Biometric Feature," MasterThesis, Vrije University, Amsterdam, 2007.
[20] J. Enrique Suarez Pascual, Jaime uriarte antonio, Raul sanchez-reillo, Michael G. lorenz, "Capturing Hand or Wrist Vein Images for Biometric Authentication Using Low- Cost Devices", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010.
[21] Xiong xianming, Chen jian, Yang surong, Cheng dapeng, "Study of Human Finger Vein Features Extraction Algorithm Based on DM6437", International Symposium on Intelligent Signal Processing and Communication Systems (lSP ACS), December 6-8, 2010.
[22] Rebecca Heyer , "Biometrics Technology Review",Defence Science and Technology Organisation (DSTO) , Edinburgh, South Australia , May 2008.
[23] Bori Toth, "Biometric Security", 2004.
[24] Griaulebiometrics website. [online] .Available: http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/introduction/applications-2.

BIOGRAPHY

Ruaa Adeeb Abdulmunem Al-falluji got the BSc in computer and information engineering from University of Mosul, Iraq, in 2006. She received the M.Sc. degree in computer and information from University of Helwan, Egypt, in 2013. Currently, she is working as Assistant Lecturer in University of Babylon, Iraq, her research interest includes Image processing, Biometrics and Pattern recognition.