BIOMETRIC SECURITY SYSTEM AND ITS APPLICATIONS IN HEALTHCARE

Harshit Jhaveri[1], Hardik Jhaveri[2], Dhaval Sanghavi[3]
[1]B.Sc [I.T.], MCA, [2]B.E. [I.T.], [3]B.E. [C.S.],
Mumbai University, Mumbai, India
[1]harshitjhaveri@gmail.com, [2]hardikjhaveri93@gmail.com, [3]dhavalsanghvi8@gmail.com

Abstract— Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. This paper is about the applications of biometric especially in the field of healthcare and its future uses.

Index Terms—Biometric security, applications, physiological, behavioral, advantages, disadvantages, biometrics in healthcare, future use.

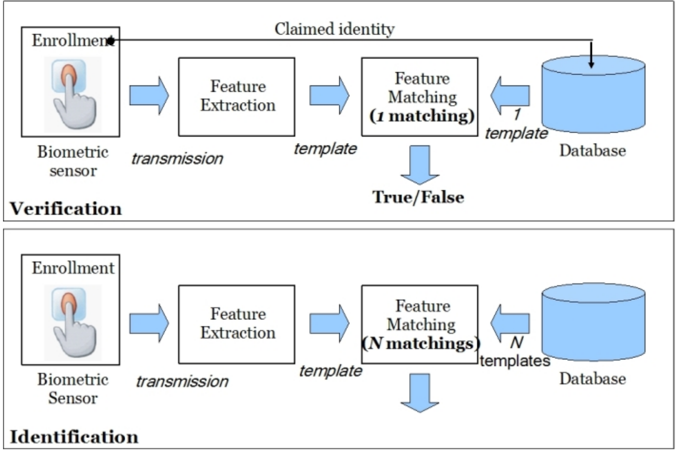
I. INTRODUCTION

Biometrics is defined as the exclusive (individual) physical/logical characteristics or behavior of human body [1]. These characteristics and behavior are used to recognize each human. Any particulars of the human body which diverges from one to other will be utilized as exclusive biometric data to provide as that individual's inimitable identification (ID), for instance retinal, iris, palm print, fingerprint, and DNA. Biometric structures will amass and lay up this data in order to employ it for confirming individual distinctiveness. The grouping of biometric data structures and biometrics authentication technologies produces the biometric security structures. The biometric security structures are a catch and confine mechanism to organize admission to particular data. In order to admittance the biometric security structure, an individual will need to provide their unique characteristics or behavior which will be matched to a database in the structure. If there is a match, the catch structure will afford access to the data for the user. The catching and confining structure will activate and record information of users who admittance the data. The association between the biometric and biometric security structure is also known as the lock and key structure. The biometrics security structure is the lock and biometrics is the key to open that lock [2].

II. WORKING

The biometric process begins with enrollment. Depending on the type of biometric being used such as physiological or behavioral data, the details are acquired and then stored in the system as a template. One of the misconceptions regarding biometrics is that the system stores all the information, whether it is a fingerprint or scan of an individual's face. In reality, depending on the system and the type of algorithms used, certain key features are extracted during enrollment and used to create a template. Each biometric vendor has its own enrollment algorithms, and some are better than others. A template can be stored locally on a PC or a network server. To verify or identify a person, an individual must present his or her biometric information to the system. A template is created and then compared to the biometric stored within the system. The act of comparing a presentation template is matched with an enrollment template called matching. When a presentation template is matched with an enrollment template, a score is generated. The score is generated based on the degree of similarity between comparisons of the two templates. A threshold number is set by the system administrator that establishes the degree of correlation necessary for a comparison between an enrollment template and a presentation template to be considered a match. Depending on the level of security desired, the threshold can be set very high or very low. To understand the impact that a threshold can have on a system, it is important to understand the concepts of the „false match rate false non-match rate, and failure to enroll rate. False match rate‟ is the probability that a user's template will be incorrectly judged to be a match for a different user's template.

Basically, this means that an imposter can succeed in logging onto the system, if the biometric information is similar to an individual already in the system. This is possible when the threshold is set very low. Changes in user's biometric data can occur. A person may get a cut or scratch on a finger. In facial recognition, a changed in hair style or glasses can affect non match rate. Therefore, no two presentation templates are the same. By raising the threshold, the system will require that presentation templates contain more biometric features than a lower threshold setting.[3]



III. CHARACTERISTICS AND PERFORMANCE

A. Characteristics

The biometrics security structure is the lock and biometrics is the key to open that lock. A set of criteria exists for this biometric security structure. There are seven basic criteria for biometric security system: uniqueness, universality, permanence, collectability, performance, acceptability and circumvention. [4]

- Uniqueness is considered as the priority one requirement for biometric data. It will indicate how differently and uniquely the biometric system will be able to recognize each user among groups of users. For instance, the DNA of each person is unique and it is impossible to replicate.

- Universality is the secondary criteria for the biometric security. This parameter indicates requirements for unique characteristics of each person in the world, which cannot be replicated. For example, retinal and iris are characteristics will satisfy this requirement.
- Thirdly, a permanence parameter is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time period. This parameter will mostly be affected by the age of the user.
- Following the permanence parameter is the collectability. The collectability parameter requires the collection of each characteristic and trait by the system in order to verify their identification.
- Then, performance is the next parameter for the system which outlines how well the security system works. The accuracy and robustness are main factors for the biometric security system. These factors will decide the performance of the biometric security system.
- The acceptability parameter will choose fields in which biometric technologies are acceptable.
- Finally, circumvention will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process. DNA is believed to be the most difficult characteristic leading to the failure of the verification process.

B. Performance

The performance or accuracy of a biometric system is data dependent usually influenced by environmental and performance factors. The environmental factors include temperature, humidity and illumination conditions around the system, whereas, the performance factors include capturing good quality images, composition of target user population, time interval between the enrollment and verification phases and robustness of recognition algorithms. However, being a pattern recognition system, the accuracy of a biometric system is usually measured in terms of sample acquisition and performance errors as described below [5]:

a) False acceptance rate or false match rate (FAR or FMR): The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FAR, which thus also depends upon the threshold value.

b) False rejection rate or false non-match rate (FRR or FNMR): The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

c) Receiver operating characteristic or relative operating characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

d) Equal error rate or crossover error rate (EER or CER): The rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.

e) Failure to enroll rate (FTE or FER): The rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

f) Failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

g) Template capacity: The maximum number of sets of data which can be stored in the system.

IV. TYPES OF BIOMETRIC SYSTEMS

Each biometric system has its own advantages and disadvantages, therefore, the question of which biometric system should be used for a given authentication application, depends on the applications requirements. A number of biometric systems have been proposed for authentication purposes. Traditionally, they can be categorized into two major groups: physical or behavioral characteristics [6].

1) Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, recognition, retina and odor/scent.

a) DNA

DNA stands for Deoxyribonucleic Acid and is a molecule that contains biological instructions of the living organisms. The DNA is composed of chemical building blocks called nucleotides. A sequence of DNA that contains information for producing a protein is known as gene, whereas the whole DNA instructions of the organisms are called genome. The human genome is shared about 99.5% to 99.9% across the human beings, however, even the small percentages of difference are of the order of millions of base pairs. The human genome is unique to each individual; however this affirmation is not valid for identical twins since they share the same DNA patterns. The low degree of popularity of this biometric characteristic is based on three factors: (1) privacy concerns, some additional information of the individual could be obtained such as diseases, (2) real-time authentication capabilities, this technique involves high computational resources and is difficult to be automated since it requires some chemical processes, and (3) access availability, it is easy to steal a piece of DNA from an individual and this information could be therefore used for fraudulent purposes.

b) Face

Face recognition is perhaps the most friendly and acceptable way to conduct human authentication. These facts rely basically on its easy collectability mechanisms and its non-intrusiveness property, e.g., people generally accept this biometric characteristic as a valid authentication method. The face recognition process often involves three different steps: (1) detect whether there exists a face in an image, (2) locate the face(s) if it is case, and (3) recognize the face(s). For each of the three mentioned steps, there are some challenges to be considered. First, face images are captured under non-controlled conditions. Therefore, these images may be characterized by the presence of different illumination conditions and backgrounds. Furthermore, changes in the facial expressions and occlusions of some facial features may reduce the overall recognition accuracy. Due to these aspects face recognition is a challenging research field.

c) Fingerprint

Fingerprints are considered nowadays one of the most reliable biometric characteristic for human recognition due to their individuality and persistence. A fingerprint consists basically on a pattern of ridges and valleys in the surface of the fingertips and its formation is related to the earlier fetal months. Maybe its main disadvantage is related to their intrusiveness, since people need to cooperate explicitly when providing their fingerprints to the system. Furthermore, fingerprint-based authentication is traditionally associated with criminal-authentication methods. State-of-the-art authentication methods have demonstrated adequate accuracies for fingerprint recognition methods, however, for the sake of human identification there are still some open tasks. First, the processing time of the current algorithms should be reduced since the output of such systems should be done in real time. Second, the non-controlled interaction between users and capture devices will produce misaligned and rotated images.

2) Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.

a) Signature

The handwriting of a given individual can be thought as representing his/her own characteristics. Signatures have been widely used in different areas ranging from government and legal applications to commercial ones. Traditionally, signature authentication may be either static or dynamic. Static signature authentication uses only the geometric features of the signatures, whereas the dynamic authentication uses not only those features, but also some additional information such as velocity, acceleration, pressure, and trajectory of the signatures. Furthermore, although it has proven reasonable authentication accuracy, it is not high enough for large-scale applications. This observation relies basically on the fact, that signatures present some variations due to the physical and emotional state of a person, and at the same time may vary over a period of time. However, such systems may be incorporated transparently since individuals are used to provide their signatures in different environments of their daily life.

b) Voice

Voice is a combination of physical and behavioral characteristics that are related to the voice signal patterns of a given individual. The physical characteristics of voice are related to the appendages that form its sound. These characteristics include for example, the vocal tracts, mouth, nasal cavities, and lips. On the other hand, the behavioral characteristics of voice are related to the emotional and physical states of the speaker.

Traditionally, voice-based authentication methods can be divided into two major groups: text-dependent and text-independent methods. In text-dependent techniques, the individuals are authenticated by speaking a fixed predetermined phrase, whereas in text-independent techniques no constraints exist about what has to be spoken. Furthermore, text-independent authentication tasks are more complex than text-dependent tasks, but they offer at the same time more reliability. Regardless of their classification type, voice-based authentication methods have to face some challenges related for example to the room acoustics, misspoken phrases or individuals emotional states. Due to all of these inconsistencies, this technique is not adequate for large-scale systems.

c) Gait

Gait is an emergent behavioral characteristic used to authenticate people by the way they walk. The attractiveness of this technique relies in its unobtrusive properties, since individuals are authenticated at certain distances without any need of big co-operation efforts. Furthermore, it has received attention from studies in medicine, psychology, and human body modeling. To create a gait signature, some models are built based on temporal and spatial metrics of the human motion. Although of its benefits, gait is not supposed to be very distinctive across individuals and therefore it is not well suited for high-security scenarios. In addition, since this technique involves video-sequence analysis, it may be computationally expensive.

V. ADVANTAGES AND DISADVANTAGES

A. Advantages

The first advantage of using this new technology is the uniqueness and it is also the main characteristic which allows biometrics technology to become more and more important in our lives. With uniqueness of biometrics technology, each individual's identification will be single most effective identification for that user. A chance of two users having the same identification in the biometrics security technology system is nearly zero.

Secondly, the highly secure way of identifying users makes this technology less prone for users to share access to highly sensitive data. For example, users can share their fingerprints, iris and so forth allowing other users access to secure information. Each trait used during identification is a single property of that user. In other words, it is extremely hard or impossible to make duplicate or share biometrics accessing data with other users. This makes it ever more secure allowing user information and data to be kept highly secure from unauthorized users.

Lastly, this identification of users though biometrics cannot be lost, stolen or forgotten. This aspect of biometrics technology allows it to become more popular in its use. This method of identifying and giving access to user makes user identification a lot easier. Finally, most biometrics security systems are easy to install and it requires small amount of funding for equipment (except modern biometrics technology such as: DNA/retinal/iris recognition) [7].

B. Disadvantages

Even though, there are many advantages of biometrics security system, it still has many flaws in its system. Each biometrics application method has weaknesses which can cause problems for its users. For example, if the biometrics security system uses fingerprints to identify its users and an accident causes a user to lose his/her finger then it can be a problem during the verification process. For voice recognition methods, illnesses such as strep throat can make it hard for authorized users to get access to their information. Another factor that can influence voice recognition systems is the continuous aging of its users. Noise in an environment where voice recognition is used to identify its users can also make it hard for users to be identified.

For iris or retinal scanning applications, users may find it very intrusive. Users may also have the concern for the safety of their eyes during the iris or retinal scan. Furthermore, databases used to store user identification data will be very large which might form a potential threat. For scanning retinal/iris characteristics and storing large amount of database, biometrics system requires new and modern technology. Therefore, the cost for equipment is also expensive. Finally, lots of people are still concerned about biometrics technology in different aspects such as: security, adaptability to rate of change in life, scalability, accuracy, privacy and others [8]

VI. APPLIATIONS

In the last years has considerably increased the area of application of biometrics and it's expected that in the near future, we will use biometry many times in our daily activities such as getting in the car, opening the door of our house, accessing to our bank account, shopping by internet, accessing to our PDA, mobile phone, laptops, etc. Depending on where the biometrics is deployed, the applications can be categorized in the following five main groups: forensic, government, commercial, health-care and traveling and immigration. However, some applications are common to these groups such as physical access, PC/network access, time and attendance, etc.

A. Forensic

a) The use of biometric in the law enforcement and forensic is more known and from long date, it is used mainly for identification of criminals. In particular, the AFIS (automatic fingerprint identification system) has been used for this purpose. Lately the facial-scan technology (mug shots) is being also used for identification of suspects. Another possible application is the verification of persons of home arrest; a voice-scan is an attractive solution for this problem. The typical applications are:

b) Identification of criminals: Collecting the evidence in the scene of crime (e.g., fingerprints) it is possible to compare with data of suspects or make a search in the database of criminals.

c) Surveillance: Using cameras one can monitor the very busy places such as stadiums, airports, meetings, etc. Looking in the crowds for suspect, based on the face recognition biometric, using a images (e.g., mug shots) database of wanted persons or criminals.

d) Correctness: This refers to the treatment of offenders (criminals) through a system of penal incarceration, rehabilitation, probation, and parole, or the administrative system by which these are effectuated. Is this cases a biometric system can avoid the possibility of accidentally releasing the wrong prisoner, or to ensure that people leaving the facilities are really visitors and not inmates.

B. Government:

There are many application of the biometry in the government sector. An AFIS is the primary system used for locating duplicates enrolls in benefits systems, electronic voting for local or national elections, driver's license emission, etc. The typical applications are:

a) Voters ID and Elections: While the biometric national ID card is still in project, in many countries are already used the biometry for the control of voting and voter registration for the national or regional elections. During the registration of voter, the biometric data is captured and stored in the card and in the database for the later use during the voting. The purpose is to prevent the duplicate registration and voting.

b) Military programs: The military has long been interested in biometrics and the technology has enjoyed extensive support from the national security community.

C. *Commercial:*

Banking and financial services represent enormous growth areas for biometric technology, with many deployments currently functioning and pilot project announced frequently. Some applications in this sector are:

a) Account Access: The use of biometric for the access to the account in the bank allows keeping definitive and auditable records of account access by employees and customers. Using biometry the customers can access accounts and employees can log into their workstations.

b) ATMs: The use of biometric in the ATM transaction allows more security.

c) Online Banking: Internet based account access is already widely used in many places, the inclusion of biometric will make more secure this type of transactions from home. Currently, there are many pilot programs using biometric in home banking.

d) E-Commerce: Biometric e-commerce is the use of biometrics to verify of identity of the individual conduction remote transaction for goods or services.

D. Travel and Immigration:

The application in this sector includes the use of biometrics to identify or verify the identity of individual interacting during the course of travel, with a travel or immigration entity or acting in the capacity of travel or immigration employee. Typical applications are:

a) Air Travel: In many airport are already used a biometric system in order to reduce the inspection processing time for authorized travelers.

b) Border Crossing: The use of biometrics to control the travelers crossing the national or state border is increasing, especially in regions with high volume of travelers or illegal immigrants.

c) Passport: Some country already issues passports with biometric information on a barcode or smart chips. The use of biometrics prevents the emission of multiple passports for the same person and also facilitates the identification at the airports and border controls.

E. Healthcare:

The applications in this sector include the use of biometrics to identify or verify the identity of individuals interacting with a health-care entity or acting in the capacity of health-care employee or professional. The main aim of biometrics is to prevent fraud, protect the patient information and control the selling of pharmaceutical products. Some typical applications are:

a) PC/Network Access: The biometrics is used to control a secure access of the employees to the hospital network, primarily, in order to protect the patient information.

b) Access to personal information: Using biometrics, the medical patient information may be stored on smart card or secure networks; this will enable the access of the patients to their personal information.

c) Patient Identification: In case of emergency, when a patient does not have identification document and is unable no communicate, biometric identification may be a good alternative to identify.

VII. BIOMETRICS IN HEALTHCARE

Healthcare system which is in the process of transformation to provide swift, safe and improved quality care is experiencing multifarious problems. In the process, the computer network is playing a very vital role and its implementation has contributed enormously but there are problems too, e.g. passwords that are meant to protect computer network systems from unauthorized use which however may also provide a false sense of security. Some use easily guessed passwords, thus facilitating unauthorized access. Patient records are vital for patient care, but incomplete health records or misplaced information or mix ups with another patient's record can result in wrong medication. In addition, if the records are in the wrong person's hand, it can lead to a great hazard to a patient's health.

We hear all the time about the mistakes that are made within our healthcare system these days. Records are mixed up, medical charts are confused, and the wrong medication is given to the wrong patient. Someone who shouldn't get their hands on your medical information does. There is a desperate race going on to find the best method of securing your data and preventing mistakes with consequences that range from embarrassing to deadly.

The healthcare sector needs an identification matching system that could help to prevent mix-ups, stop patient identity fraud, eliminate the creation of duplicate medical records, and reduce billing errors. As a solution, biometrics with its distinct advantages in patient identification speed, accuracy, hygiene, real-time de-duplication search capability, and data standardization is being used nowadays.

VIII. BIOMETRICS – AN IDEAL SOLUTION

The problems of current healthcare systems regarding Health Care Fraud, Health Endangerment, wastage of resources, payment issues, patient information security, inventory thefts, errors due to incomplete records, falsified medical reports, leakage of sensitive information etc lead to less safe and efficient patient care. Some applications of biometrics in this field are as follows: [9]

- Assists providers to obtain faster payments for services rendered by verifying at the provider's location that a patient is eligible at the time of service.
- Reduces the costs and risks associated with the payment programs that attempt to recoup inaccurate and fraudulent payments.
- Increases patient safety by reducing medical errors due to mismatched or incomplete records. The unique biometric identifier ensures an accurate match to their electronic health care record under most care conditions.
- Provides a unique and more accurate patient and provider master index to ensure that patient records in multiple provider locations can be linked accurately. This increases the usefulness of electronic health records, their safety and privacy.
- Protects patient identity and patient health care information by providing an efficient and convenient means of authenticating both patients and providers before allowing access to records.
- In health care programs, where individuals' eligibility for certain services often changes, biometrics also would be able to verify that the individual requesting treatment is eligible or not. This information would obviously be of great value to patients and providers.
- Reduces costs and eliminating 'inventory theft' for example securing medication cabinets through biometric access can provide accurate audit trails detailing what individuals accessed the inventory. This is proven to reduce inventory loss and theft.
- Creating an 'audit trail' for check in and checkout times for comparison against type of service provided as an indicator of potential fraud called 'upcoding'.
- Preventing card sharing and patient identity theft by authenticating the patient in the provider's location.
- It can help in detecting the disease while the number of seriously ill individuals provides a short interval to initiate aggressive treatment and prophylaxis measures that, if effective, would substantially reduce the mortality, morbidity and resource requirements.

IX. FUTURE OF BIOMETRICS

There are numerous healthcare applications which have or will benefit from the implementation of biometrics. These include, but not limited to clinics, Intensive Care Units, Newborn nurseries, general and specialty care areas, admitting, pharmacy (electronic prescription), staff, time attendance, medical record management etc.

Everyone recognize that human lives depend on shared medical data and information and any effort to effectively share information requires a trusted health data exchange. Security is always a vital concern when it comes to confidential medical data and must be balanced with convenient access to patient records. Another key issue for adoption of biometrics is privacy which is of paramount importance. It is fair to say that any biometric solution that implants an actual physical identifier in a patient record must adhere to stringent regulatory requirement that protect the patient's privacy in the event of compromise.

The biometric plays a very important role in not only in maintaining privacy and security of healthcare management system but is of tremendous value in public health activities in notifying infectious diseases and controlling mortality and morbidity rates by linking with curative hospitals.

Biometric technology represents the future for positive healthcare identification and will enhance the secure use, storage, and exchange of personal health information. The use of biometrics to secure patient and provider identities can prevent certain health care fraud, thus increasing the efficiency and effectiveness of health care programs.

X. CONCLUSION

Biometrics is a very interesting and exciting field that has be growing exponentially in recent years. The wide variety of physically unique traits our bodies give us will soon allow us to live in a very secure password-less world. There are many applications and solutions of biometrics technology used in security systems. It has many advantages which can improve our lives such as: improved security and effectiveness, reduced fraud and password administrator costs, ease of use and makes live more comfortable. Even though the biometrics security system still has many concerns such as information privacy, physical privacy and religious objections, users cannot deny the fact that this new technology will change our lives for the better.

ACKNOWLEGMENT

We would like to thank our parents Mr. Ketan Jhaveri, Mrs. Bina Jhaveri, Mr. Rohit Sanghavi and Mrs. Sudha Sanghvi for their love, support and encouragement during all times and for always believing in us.

References

[1] Jain, A.K.;Ross, A.;Prabhakar, S.;"An introduction to biometric recognition", Volume: 14 Issue: 1 Issue Date: Jan. 2004, on page(s): 4 - 20

[2] Jain, A.K.; Ross, A.; Pankanti, S., "Biometrics: a tool for information security" Volume: 1 Issue: 2, Issue Date: June 2006, page(s): 125 - 143 J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] Role of Biometrics in healthcare privacy and security management, Sri Lanka Journal of Bio-Medical Informatics 2011;2(4):156-165

[4] A Survey of Biometrics Security Systems, cse571-11

[5] "CHARACTERISTICS OF BIOMETRIC SYSTEMS". Cernet.

[6] Book-Understanding-biometrics, griaulebiometrics.

[7] Massimo Tistarelli and Marks Nixon, "Advances In Biometrics", Springer-Verlag Berlin Heidelberg 2009, ISBN 03029743

[8] "Advantages and Disadvantages of technologies", 2006 http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies

[9] International Biometrics and identification association, IBIA, US