INTERNATIONAL JOURNAL OF
INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211

Biometric Authentication System

Prof.Shital Parasmal Bora

&

Prof.Pankaj B. Dhumane

Sardar Patel College, Chandrapur (M.S)
India

Abstract:

This paper covers the field of biometric systems focus on biometric authentication systems. A short and general overview of biometric authentication systems gives some insight in how the various biometric data can be used for authentication. The problems of varying biometric data, caused by noise respectively human nature and approaches to solve these problems with multi-biometric systems in combination with information fusion, are also discussed. Since there is such a vast range of variances for the usage of biometric systems, some type of statistics is determined.

Keywords: Authentication, biometric, identification, verification.

Introduction:

First of all the term Biometrics should be more or less defined in order to have a common understanding of the subject. Both terms ”Biometrics” and ”Biometry” have been used since early in the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. Recently the term Biometrics has also been used to refer to the emerging field of technology devoted to identification of individuals on the basis of their biological traits, such as those based on retina-scans, iris-patterns, fingerprints or face recognition. The recent usage and meaning of the term Biometrics will be the primary focus of this paper. In today’s world a wide variety of applications requires reliable and secure authentication methods to confirm the identity of an individual requesting their service. Some examples of such applications would include secure access to buildings, computer systems, laptops, cellular phones, memory such as USB sticks and many more. Furthermore it is possible to establish an identity based on who you are rather than by what you posses. (e.g. identification cards) or what you remember. (e.g. passwords).

Biometric System Examples

FINGERPRINT

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. The fingerprint itself consists of patterns found on the tip of the finger, thus making it a physical biometric. Fingerprints are known to be unique and immutable for each person and the basic characteristics of fingerprints do not change with time. The uniqueness of a fingerprint can be determined by the patterns of ridges and furrows as well as the points on the surface of the finger. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprints are routinely used in forensic laboratories and identification units all over the world and have been accepted in the court of law for nearly a century. Since the 1980's the usage of fingerprints in civil areas has become more relevant because of increasing accuracy and decreasing prices of fingerprint devices. Some examples of the use of fingerprint devices in civil areas are: Permitting logins based on fingerprints.

HANDSCAN

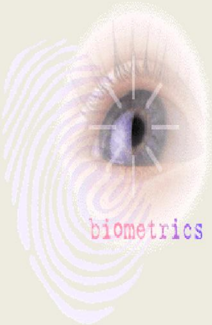
This biometric approach uses the geometric form of the hand for confirming an individual's identity. Specific features of a hand must be combined to assure dynamic verification, since human hands are not unique. Characteristics such as finger curves, thickness and length, the height and width of the back of the hand, the distances between joints and the overall bone structure, are usually extracted. Those characteristics are pretty much persistent and mostly do not change in a range of years. The verification process requires the user to enter an ID in order to verify the claimed identity. After the user ID has been entered and the photos have been captured, the calculation of the feature set representing the biometric trait and the verification process lasts no longer than a second. Handscan applications have proven their practical use which is shown by the 30-60% market share of biometric identification applications.

SIGNATURE

Signature verification is the process used to recognize an individual's hand-written signature. Dynamic signature verification uses behavioral biometrics of a hand written signature to confirm the identity of a person. This can be achieved by analyzing the shape, speed, stroke, and pen pressure and timing information during the act of signing. On the other hand there is the simple signature comparison which only takes into account what the signature looks like. So with dynamic signature verification, it is not the shape or look of the signature that is meaningful, it is the changes in speed, pressure and timing that occur during the act of signing, thus making it virtually impossible to duplicate those features. Devices which enable dynamic signature verification store the behavioral factors and the captured signature image itself for future comparison in their database. These devices account changes in one's signature over time by recording the time and the dynamic features each time a person uses the system. The major difficulty with this technology is to differentiate between the consistent parts of a signature; these are the characteristics of the static image, and the behavioral parts of a signature, which vary with each signing. Comparing many signatures made by one individual reveals the fact that an individual’s signature is never entirely the same and can vary substantially over an individual's lifetime. Allowing these variations in the system, while providing the best protection against forgery is a big problem faced by this biometric technology. The financial industry sometimes uses signature verification for money transactions.

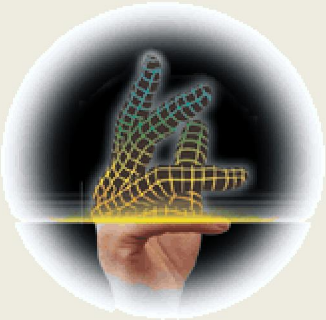
IRIS

Iris scan biometrics employs the unique characteristics and features of the human iris, which remains unchanged throughout an individual's lifetime, in order to verify the identity of an individual. The iris is the area of the eye where the pigmented or colored circle, usually brown, green, grey or blue, rings the dark pupil of the eye. The iris is well protected cause of the human anatomy and therefore injuries are rare. Typically the iris scan process begins with a photograph which is taken with a special camera close to the subject. The user has to be in between a maximum distance of about 1 meter to the reading device. The camera uses an infrared imager to illuminate the eye and capture a very high resolution photograph. The inner edge of the iris is located by an iris-scan algorithm which maps the iris distinct patterns and characteristics. Systems using iris biometrics even work with glasses and this technology is one of the few biometric technologies that can work well in identification mode. Iris patterns are extremely complex, carrying an astonishing amount of information and have over 200 unique spots. Unique spots are categorized into the tissue, which gives the appearance of dividing the iris in a radial fashion, rings, furrows, freckles and the corona. The fact that an individual's right and left eyes are different and that patterns are easy to capture, establishes iris-scan technology as one of the biometrics that is very resistant to false matching and fraud.

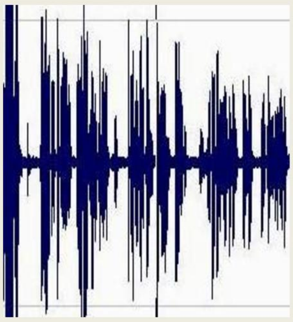


(a) Retina

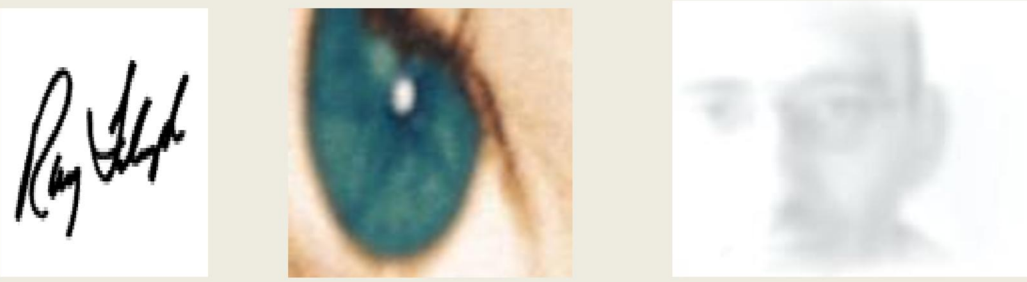
(b) Fingerprint



(c) Hand geometry



(d) Voice



(e) Signature (f) Iris (g) Facial

Fig. 1. Examples of some of the biometric traits associated with an individual: (a) Retina (b) Fingerprint, (c) Hand geometry, (d) Voice (e) Signature (f) Iris (g) Facial

RETINA

Along with iris recognition technology, retina scan is perhaps the most accurate and reliable biometric technology. It is also among the most difficult to use and requires well trained, and is perceived as being moderately to highly intrusive. The users have to be cooperative and patient to achieve a proper performance. Basically the retina, a thin nerve on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain. Blood vessels used for biometric identification are located along the neural retina which is the outermost of the retina's four cell layers from person to person. It has even been proven that these patterns, even between identical twins, were indeed unique. This pattern also doesn't change over the course of a lifetime. Retinal scanners require the user to place their eye into some sort of device and then ask the user to look at a particular spot so that the retina can be clearly imaged. This technology involves using a low-intensity infrared light source through an optical coupler to scan the unique patterns of the retina. The reflection of the vascular information is being recorded. Retina scanning works well in modes, identification and verification. Additional advantages include the small template size and good operational speed.

VOICE

Of the many types of biometric technologies available today, voice identification and authentication solutions have a unique edge over much of the competition, because customers typically don't need to purchase new hardware to implement the solutions.

Most of the voice biometric solutions can be used through a typical telephone or microphone hooked up to the computer. In order to identify or authenticate users, most voice biometric solutions create a voice print of the user, a template of the person's unique voice characteristics created when the user enrolls with the system. During enrollment the user has to select a passphrase or repeat a sequence of numbers. The passphrase should be in the length of 1 to 1.5 seconds. The problem with shorter passphrases is that they have not enough data for identification. Longer pass phrases have too much information. The user has to repeat the passphrase or the sequence of numbers several times. This makes the enrollment process lasting much longer than with other biometric technologies. All subsequent attempts to access the system require the user to speak, so that their live voice sample may be compared against the pre-recorded template. A voice biometric sample is a numerical model of the sound, pattern and rhythm of an individual’s voice. A problem considering the voice is that people's voices change over time along growth, or when someone has got a cold or another disease. Background noise can also be a disturbing factor.

FACE

Human face detection plays an important role in applications such as video surveillance, human computer interfaces, face recognition, and face image databases. To enable this biometric technology it requires having at least a video camera, PC camera or a single-image camera. Nevertheless, this biometric approach still has to deal with a lot of problems and cannot work with acceptable identification rates unless certain restrictions are being considered. Finding a face in a picture where the position, the orientation, the background and the size of a face is variable is a very hard task and many algorithms have been worked on to solve this problem. Other problems with face detection occur whenever faces are partially covered, as with beards, glasses, hair style or hats, because a lot of information just stays hidden.

Biometric Authentication Systems

Looking at biometric systems in a more general way will reveal certain things all biometric-based authentication systems have in common. In general such systems work in two modes:

ENROLLMENT MODE

In this mode biometric user data is acquired. This is mostly done with some type of biometric reader. Afterwards the gathered information is stored in a database where it is labeled with a user identity (e.g. name, identification number) to facilitate authentication.

AUTHENTICATION MODE

Again biometric user data is acquired first and used by the system to either verify the users claimed identity or to identify who the user is. While identification involves the process of comparing the user's biometric data against all users in the database, the process of verification compares the biometric data against only those entries in the database which are corresponding to the users claimed identity. In general one can consider the verification of the identity of a person a two-class problem: either the person is who he/she claims to be (client) or the person fails to be the one he/she claims to be (impostor) So we are basically dealing with a binary-decision scheme where we either accept or reject a person. Simple biometric systems usually consist of the following four components:

Sensor modules: This module acquires biometric user data. Examples of sensor modules would be an retina scanner or a fingerprint sensor.

Feature extraction modules: This module is responsible for extracting feature values of a biometric trait. If hand geometry would be used as a biometric trait then feature values would include width of fingers at various locations, width of the palm, thickness of the palm, length of fingers etc.

Matching modules: The matching modules compare the acquired biometric features against those stored in a database.

Decision-making modules: The user's identity is either established or a claimed identity is accepted or rejected. This is done based on the results of the matching modules. Since we are dealing with a binary decision scheme it is obvious that the decision-making module can make two kinds of errors. The errors, which can be made in the process of verification, are called:

False Rejection (FR): when an actual client gets identified as an impostor

False Acceptance (FA): when an actual impostor gets identified as a client.

Performance Evaluation

The performance of a biometric authentication system can be measured as the False Acceptance Rate FAR Equation (2), or the False Rejection Rate FRR Equation (1) which are defined as:

FRR = number of false rejections/number of client accesses ----(1)

FAR =number of false acceptances/number of client accesses ----(2)

A perfect biometric authentication system would have a FRR = 0 and a FAR = 0 which is a little bit unachievable in reality. It is also interesting that any of the two values FRR and FAR can be reduced to an arbitrary small number, with the drawback of increasing the other value. Another interesting value is the Total Error Rate TER Equation (3) which is defined as:

TER =number of FA + number of FR/total number of access----(3)

At this point it is important to emphasize the fact that these measures could be heavily biased by one or either type of errors (FAR or FRR) depending only on the number of accesses which have been used in obtaining these respective errors. This means that the TER will always be closer to that type of error which has been obtained with the largest number of accesses. The overall performance of a biometric authentication system should not be measured by the TER but rather by the Receiver Operation Characteristic ROC, which represents the FAR as a function of the FRR.

Problems With Biometrics

In theory collecting and verifying biometric data is no problem but in today's demanding real-world applications there are a lot of problems with biometric systems. One of those problems is that biometric traits extracted from persons tend to vary with time for one and the same person and to make it even worse, this variation is itself very variable from one person to another. Most of the other problems are caused by extreme or constantly changing surroundings and the nature of certain biometric measures.

NOISE

Noisy biometric data like a person having a cold (voice recognition), a simple cut on ones finger (fingerprint scan) or different lighting conditions (face detection) are some examples of noisy inputs. Other examples are misconfigured or improperly maintained sensors or inconvenient ambient conditions like dirt on a sensor for fingerprints or voice recognition with loud background noise. The problem with noisy biometric data is that authorized personnel may get incorrectly rejected(FR), if the noisy data affects the extracted features so much, that no match can be found in the biometric database. The other extreme situation would occur if noise would change the extracted features in such a way, that the result feature set would match to another person (FA).

DISTINCTIVENESS

While a biometric trait is expected to vary significantly across individuals, there may be large similarities in the feature sets used to represent theses traits. Thus, every biometric trait has a theoretical upper bound in terms of discrimination capability.

NON-UNIVERSALITY

The problem of non-universality arises when it is not possible to acquire certain biometric traits from all users. That means that even though a person has a fingerprint, it still may be impossible to acquire that trait because of the poor quality of the ridges which make up the fingerprint.

Multi Biometric Systems

Most of the problems and limitations of biometrics are imposed by unimodal biometric systems. Unimodal biometric systems rely on the evidence of only a single biometric trait. Some of these problems may be overcome by multi biometric systems and an efficient fusion scheme to combine the information presented in multiple biometric traits. It is evident that problems like non-universal traits, distinctiveness and security problems are easier and better to deal with if more biometric traits are present. So if a person’s fingerprint cannot be acquired by a sensor, other biometric methods like voice recognition and retina scans are taken into account and the resulting data is validated against the biometric database.

FUSION OF BIOMETRIC DATA:

In general there are three possible levels of fusion for combining two or more biometric systems to a multi biometric system:

Fusion at the feature extraction level:

Feature sets are acquired from each sensor where each feature set is represented as a vector. Then the vectors are concatenated which results in a new feature vector with higher dimensionality representing a person’s identity in a different hyperspace.

FUSION AT THE MATCHING SCORES LEVEL:

Each biometric system provides a matching score which indicates the proximity of the feature vector with the template vector. Fusion at this level would mean combining the matching scores in order to verify the claimed identity. In order to combine the matching scores reported by the sensors, techniques such as logistic regression are used. These techniques attempt to minimize the FRR for a given FAR.

FUSION AT DECISION LEVEL:

The resulting feature vectors from each sensor need to be classified into two classes - reject or accept. Biometric terms, such as recognition, verification and identification, are sometimes used randomly. This is not only confusing, but incorrect as each term has a different meaning. Recognition is a generic term and does not necessarily imply either verification or identification. All biometric systems perform "recognition" to "again know" a person who has been previously enrolled. Verification is a task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates. Identification is a task where the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine if the person is in the database. Because of these variances, different statistics must be used for each task.

Conclusion:

Biometric systems and especially multi biometric systems have a huge potential of growth. By using biometric technologies, access procedures should be made simpler, faster and more secure. Especially governments, law enforcement agencies, military and industrial companies, already make partial use of this technology. In the future biometric devices will surely become more involved in many civil areas. Maybe in a couple of years access to ones private home or car will be granted upon a successful iris scan, thus making the traditional house or car keys obsolete.

Maybe money, credit cards and cheques will become obsolete by leaving ones fingerprint instead of a certain amount of monetary value. But in spite of all the advantages coming along with the broader usage of biometric technology in our everyday lives, this technology also brings up a whole new range of difficulties and problems. So it will not suffice to study factors like cost versus performance tradeoffs, or usability and security issues before deploying biometric systems. Very special care must be taken what may be done with the acquired biometric data and who may use it for a certain purpose.

References:

1. A. K. Jain, A. Ross. .Mutlibiometric Systems., Communications of the ACM, Vol. 74, pp. 34-40, 2004.
2. A. K. Jain, A. Ross. .Information fusion in biometrics., Pattern Recognition Letters, Vol. 24, pp. 2115-2125, 2003
3. A.K. Jain, S. Prabhakar, S. Chen. .Combining multiple matchers for a high security fingerprint verification system., Pattern Recognition Letters, Vol. 20, pp. 1371-1379, 1999
4. M. Roach, J.D. Brand, and J.S.D. Mason. .Acoustic and Facial Features for Speaker Recognition., ICPR, 2000.
5. P. Verlinde, M. Acheroy. .A Contribution to Multi-Modal Identity Verification Using Decision Fusion., Decision Fusion. ENST-Paris Ph.D. Thesis, 1999.
6. S. Liu, M. Silverman. .A Practical Guide to Biometric Security Technology.www.computer.org/itpro/homepage/JanFeb/security3.htm, 2000