ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

A Comparative Study of Biometric Techniques

Shibani Kulkarni, Neeta Takawale

Asst. Professor, Dept of Computer Science, Dr. D. Y. Patil ACS College, Pune, India.

ABSTRACT : In today's world data security is a major issue ,there are numerous methods to secure data or prevent unauthorized access Biometrics is a rapidly evolving technology that is being widely used in forensics, security; prevent unauthorized access in bank or ATMs. There are numerous forms of biometrics now being built into technology platforms. As biometric technology evolves there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the technology, user acceptance, and the credibility of the service provider. In this paper we present a brief introduction of biometric system, applications and we have studied and compared five biometric techniques along seven factors.

KEYWORDS : Biometric techniques, recognition, verification and identification.

I. INTRODUCTION

There has been a tremendous change in the use and applications of science and security of which biometrics is one the most widely discussed and experimented field. Biometrics has undergone drastic changes since its first inception as a Fingerprint recognizing method in China in the 14th century. Later on finger printing has become more standardized making it a gateway for other techniques like Finger, Iris, Voice Recognition, face recognition and many more. In the recent years, a number of recognition and authentication systems based on Biometric measurements have been proposed. Biometrics is going to be the most happening of all technologies in the field of Security.

There are many biometric techniques being used today and many new approaches are still in the early stages of development. Biometrics can, therefore, be grouped into two categories: those that are currently in use across a range of platforms and those still in limited use or still in the stage of development.

II. LITERATURE REVIEW

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses. A biometric system typically operates in one of two modes depending on the application context i. e. verification or identification.

Verification mode : A person's identity is validated by comparing the captured biometric characteristic with the individual's biometric template, which is prestored in the system database. In such a system, an individual who desires to be recognized claims an identity—usually via a personal identification number (PIN), login name, smart card, or the like—and the system conducts a one-to-one comparison to determine whether the claim is true. Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

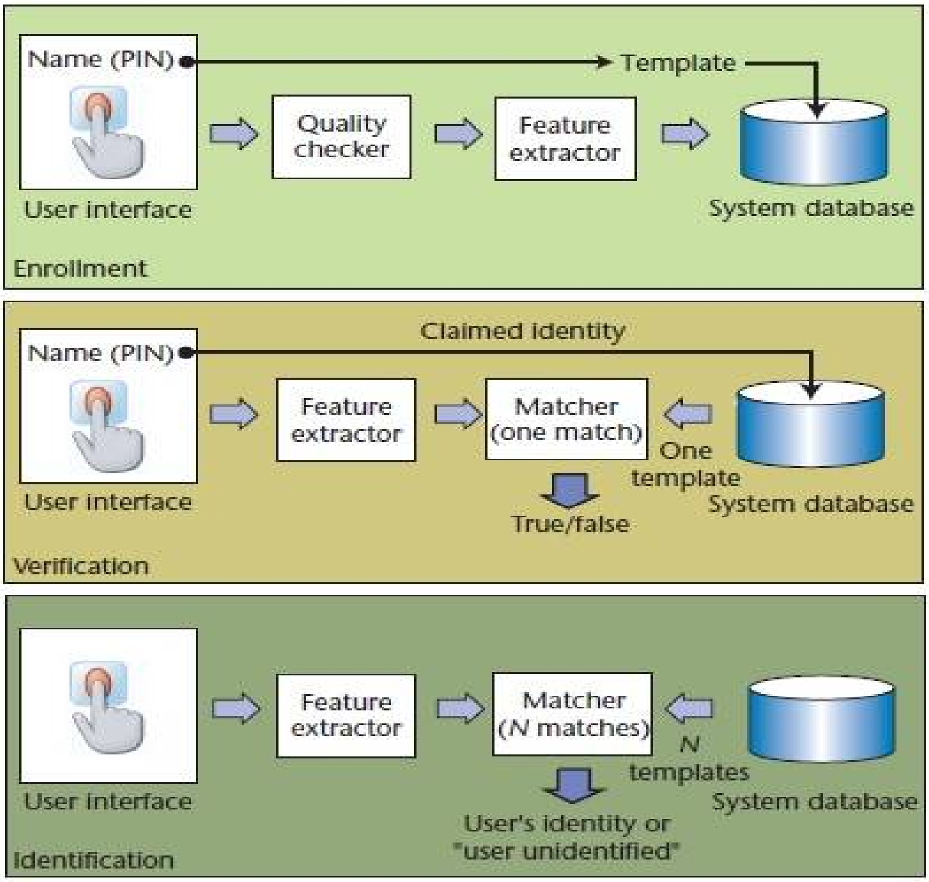
Identification mode: Identification is a critical component of negative recognition applications, in which the system establishes whether the person is who she/he denies being. The system recognizes an individual by searching the entire template database for a match. The system conducts a one-to-many comparison to establish an individual's identity. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification can also be used in positive recognition for convenience. While the traditional methods of personal recognition such as passwords, PINs, keys, and tokens work for positive recognition, only biometrics can be used for negative recognition.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016



Block diagrams of a verification system and an identification system, both performing the task of user enrollment.

The enrollment module registers individuals into the biometric system database. During the enrollment phase, a biometric reader first scans the individual’s biometric characteristic through fingerprint or camera to produce its digital representation. The system generally performs a quality check to ensure that successive stages can reliably process the acquired sample. To facilitate matching, a feature extractor processes the input sample to generate a compact but expressive representation, called a template. Depending on the application, the biometric system might store the template in its central database or record it on a smart card issued to the individual.

III. BIOMETRIC SYSTEM ERRORS

A biometric verification system can make two types of errors:

- Mistaking biometric measurements from two different persons to be from the same person (called false match or false accept)
- Mistaking two biometric measurements from the same person to be from two different persons (called false non-match or false reject)

There are some reasons behind biometric verification system errors as two samples of the same biometric characteristic from the same personare not exactly the same because :

- imperfect imaging conditions
- changes in the user’s physiological or behavioral characteristics
- ambient conditions
- the user’s interaction with the sensor

A threshold t regulates the system decision. The sys-tem infers that pairs of biometric samples generating

DOI: 10.15680/IJIRCCE.2016. 0401060

scores higher than or equal to t are mate pairs that is, they belong to the same person. Consequently, pairs of biometric samples generating scores lower than t are nonmate pairs that is, they belong to different persons.

IV. APPLICATIONS OF BIOMETRIC SYSTEMS

Biometric applications fall into three main groups:

- Commercial applications: Biometric device is used in various commercial applications such as computer network logins, electronic data security, e-commerce, Internet access, ATMs, credit cards, physical access control, cellular phones, PDAs, medical records management, and distance learning
- Government applications: There are some government sectors that widely make use of biometric applications such as national ID cards, correctional facilities, driver's licenses, social security, border control, passport control, and welfare-disbursement.
- Forensic applications: such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

In the commercial category, applications require positive recognition and may use the biometric system either in verification or identification mode.

A. Positive recognition: Commercial applications

Traditional technologies available for achieving a positive recognition include knowledge-based methods, for example, PINs and passwords and token-based methods such as keys and cards. Such Possession-based personal recognition suffers from many problems such as keys and tokens can be shared, duplicated, lost, or stolen, or an attacker could make a master key that opens many locks. But it is significantly difficult to copy, share, or distribute biometrics.

Biometrics cannot be lost or forgotten, and online biometrics-based recognition systems require the person being recognized to be present at the point of recognition. Biometrics is difficult for attackers to forge and for users to repudiate. Furthermore, the security level is relatively equal for all users in a system, which means that one account is no easier to break than any other (for example, through social engineering). The main advantage of a biometric system is that it gives users greater convenience (they no longer have to re-member multiple, long and complex, frequently changing passwords) while maintaining sufficiently high accuracy and ensuring that the user is present at the point and time of recognition.

B. Negative recognition: Government and forensic applications

Negative recognition applications, such as background-checking of employees and preventing terrorists from boarding airplanes, must perform personal recognition in identification mode. As we noted earlier, at a given level of accuracy, identification is a much harder problem than verification because an identification system must per-form a large number of comparisons.

The semiautomatic biometric applications are more cost effective, as the system only generates an alarm that calls for a closer, manual examination of the individual.

Other negative recognition applications, such as back-ground checks and forensic criminal identification, can also operate in semiautomatic mode, and their use follows a similar cost-benefit analysis. For example, in attempting to match latent fingerprints, law enforcement agencies typically use an automatic fingerprint identification system (AFIS) only to narrow down the number of finger-print matches from a few million to a few hundred for a human expert to perform. A forensic expert always makes the final decision.

V. COMPARISON OF BIOMETRIC TECHNIQUES

A. Fingerprint recognition:

Fingerprint is a pattern of ridges and valleys on the surface of the fingerprint. These patterns of ridges are of three types i.e. arch, loop and the cycle

i. Loop: the ridges enter from one side of finger, from a license, password curve, and exit on same side.
ii. Arch: the ridges enter from one side of finger, rise in the center forming an arc, and exit the other side of finger.
iii. Whorl: ridges form circularly around the central point of finger.

Fingerprint is highly reliable, robust, accurate and highly distinctive method of verification. Fingerprint is user convenient. It is also stable over time. There are some disadvantages in fingerprint capturing. Functional defects are possible if the fingertips are very dirty or worn. Injury to fingertip also cause defect. Dry skin, grease and sweat person's fingerprints are difficult to recognize.

B. Voice recognition:

The voice is a unique feature of every individual. Using voice recognition it is possible to identify a user from the existing database by utilizing the unique features of the voice including the pitch, time, amplitude, intensity. The acoustic pattern reflects the behavioral patterns. Voice is compared with a previously created voice print. The system also compares the characteristics of lip motions while person speaks. This will help in identification associated with speaker.

C. Face recognition:

Face recognition is a non-intrusive method, and facial images are probably the most common Biometric characteristic used by humans to recognize a person. The most popular approaches to face recognition are based on either the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or the relationships, or canonical faces. In order that a facial recognition system works well in practice it should automatically detect whether a face is present in the acquired image; locate the face if there is one; and recognize the face from a general view point . The system uses an image or series of images either from a camera or photograph to recognize a person. The face from a digital image or from a video source is matched with the existing database.

D. Palm recognition:

The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. Palm print scanner is needed to capture a large area, they are more expensive than the fingerprint sensor. Human palms also contain additional distinctive features such as principle lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper. When using a high resolution palm print scanner, all the features as hand geometry, rides wrinkles, and valley can be combined to build a highly accurate biometric system. It is a 3-dimentional image of hand from which extracted features are compared with the database feature vectors. These features are bulky but identification is done in short time.

E. Iris

Iris is an individually unique ring-shaped coloured area around the pupil. Its complex texture is stabilized by the age of 2 and does not change throughout one's life unless an eye has experienced some physical trauma No two iris structures are alike, even in the case of identical twins. Advantages of iris based system are,

- Absolutely non-intrusive data collection.
- Data capturing can even be performed if the user is wearing glasses or contact lenses.
- No need to keep a certain distance from the biometric reader or focus the eyes on a target system.
- High speed of recognition and accuracy.
- Easy detection of fake irises.

The following table compares five biometric techniques along seven factors :

Biometric	Uniqueness	Universality	Permanence	Circumvention	Performance	Collectablity	Distinctive
Fingerprint	G	A	G	A	G	A	G
Voice	P	A	P	G	P	A	P
Face	L	G	A	G	P	G	P
Palm	A	A	G	M	G	A	A
Iris	G	G	G	P	G	A	G

(Comparison of trends based on various criteria
P=poor, A=average, G=good. Source: Biometric Wikipedia)

DOI: 10.15680/IJIRCCE.2016. 0401060

VI. CONCLUSION

We have used rating scale method in above table like P=Poor, A=Average, G=Good to rate and compare the five biometric techniques along seven factors. From the study of various biometric techniques and in particular the five biometric techniques that we studied in this paper along seven factors we would like to present the following observations.

- Several biometric characteristics are in use in various applications. Each biometric has its strengths and weaknesses, and the choice typically depends on the application.
- No single biometric can effectively meet the requirements of all applications—none is “optimal.”
- We match a specific biometric to an application depending on the application’s operational mode and the biometric characteristic’s properties. For example, both the finger-print- and iris-based techniques are more accurate than the voice-based technique. However, in a telebanking application, the voice-based technique might be preferable because the bank could integrate it seamlessly into the existing telephone system.

REFERENCES

1. www.sciencepublication.org/ijast/documents/ijastiss2/4.pdf.
2. http://www.ijcaonline.org/volume14/number5/pxc3872493.pdf.
3. http://mms.ecs.soton.ac.uk/2011/papers/4.pdf.
4. http://www.biometrics.gov/documents/biotechstandard.pdf.
5. http://iasir.net/IJETCASpapers/IJETCAS14-598.pdf.
6. http://www.bioconsulting.com/bio.htm.
7. http://www.biometrics.gov/referenceroom/introduction.aspx.
8. https://en.wikipedia.org/wiki/Biometrics.

DOI: 10.15680/IJIRCCE.2016. 0401060