Different Kind of Biometrics Technique

Prashant Kumar
Department of Electronics and Communication Engineering
Faculty of Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

ABSTRACT: Biometrics is an electronic tool for recognizing an individual or for verifying a person's identification based on a physiological or behavioural attribute that is capable of accurately discriminating between an authenticated individual and an impostor. Because biometric identifiers are identifiable, cannot be ignored or misplaced, and at the point of authentication, the individual to be authenticated has to be physically present, biometrics is potentially more accurate and efficient than conventional knowledge-based and token-based techniques. Common Biometrics Safety has become a crucial and challenging problem in the modern era of digitization not just for the departments of defence or government, but also for a regular guy, as today it is very much reliant on computers that authenticate the user by any identification to enable them to be used. Biometric Systems are automatic mechanisms for checking or identifying a living person's identification based on certain anatomical features, such as a fingerprint or facial image, or certain behavioural attributes, such as signature or keypad patterns.

KEYWORDS: Biometric, Face Recognition, Finger Print Scanner, Iris Recognition, Voice Scanner.

INTRODUCTION

The concept "biometrics[1]" comes from the Roman terms bio (life) and metric (to count). Biometrics refers to techniques that quantify and interpret the physiological or behavioural features of an individual for our usage. These features are special to individuals, and may therefore be used to validate or classify a person. Biometrics, defined as the science of identifying a person[2] on the basis of his or her legal method of identity determination. Biometrics is the automated manipulation of physiological or behavioural properties to establish or validate identification Biometrics, which refers to the recognition of a person based on its physiological or behavioural features. Physiological traits include depictions of the hand or the eye, facial appearance and identification of the iris. Behavioural features are lessons gained or developed attributes. Verification of complex signatures, speech verification, and keystroke patterns. There's no one biometric right that suits any need. Both biometric devices have their own pros and cons. Nonetheless, there are several specific features needed to render a biometric device functional.

Second, there must be a distinguishable attribute of the biometric. Most experimental research reinforces the theory that "no two fingerprints are identical." Techniques such as hand mechanics have been utilized for many years and techniques such as facial recognition or iris detection have come into common usage. Many newer biometric approaches might be as reliable, but further work will be required to determine their uniqueness. Another main thing is the fact a program is "user friendly." The procedure will be fast and simple, such as getting a video camera photo taken, speaking in a microphone or pressing a fingerprint scanner. Low cost is crucial because most implementers recognize that it's not just the sensor's initial expense or matching applications involved. The life-cycle maintenance costs of program management and an enrolment operator will always exceed the initial biometric hardware costs. The benefit of biometric security is the potential to allow more instances of security in such a simple and convenient manner that the extra criteria don't annoy people. When biometric solutions evolve and fall into wide commercial usage, coping with multiple authentication rates or multiple authentication instances may become less of a hassle for users. Biometrics has been commonly used in applications of forensics such as suspect detection and prison defence. Biometric technology is developing quickly and has a very high potential to be broadly adopted in civilian applications such as online banking, e-commerce and access control[3].

Mobile banking and online trading are now one of the most significant new uses of biometrics, leading to a growing growth in the amount and use of electronic transactions. Biometrics has been commonly used in applications of forensics such as suspect detection and prison defence. Biometric technology is developing quickly and has a very high potential to be broadly adopted in civilian applications such as online banking, e-commerce and access control. Mobile banking and online trading are now one of the most significant new uses of biometrics[4], leading to a growing growth in the amount and use of electronic transactions. Biometric authentication involves comparing a biometric sample recorded or enrolled (biometric blueprint or identifier) to a freshly captured biometric sample (for example, a fingerprint captured during login). A snapshot of the biometric characteristic is collected during Enrolment, analysed by a computer, and retained for future reference. Biometric identification may be used in Identification mode, where an individual from the whole enrolled population is detected by the biometric device through looking for a match based solely on biometrics. A device can often be used in Authentication mode, where the biometric method authenticates the reported identification of an individual from their template previously enrolled. This is often called matching “one-to- one”.

DIFFERENT TYPE OF BIOMETRIC

Face Recognition:

Facial recognition is a biometric application of software[5] that can uniquely recognize or validate an individual by matching and analysing trends based on the facial contours of the human. Facial recognition is mainly used for protection purposes but concern in other fields of usage is growing. In reality, facial recognition technology has gained considerable interest because it has the ability for a wide variety of law enforcement specific uses as well as many companies. A person's recognition by their facial expression may be achieved in a variety of various forms, such as taking a face picture in the visual range with a cheap camera or utilizing the facial heat emission infrared patterns. Face detection usually model main aspects of the central portion of a facial expression in visible light. The visible light systems derive characteristics from the filmed image(s) using a large variety of cameras that do not alter with time while eliminating trivial aspects such as facial gestures or hair. Several methods to visible spectrum facial image processing include Principal Component Analysis, Spatial Feature Analysis, Neural Networks, Elastic Graph Theory, and Multi-Resolution Analysis Some of the problems in visual spectrum facial recognition involve the effect in ambient illumination, and identifying a mask or object. Some facial recognition systems that allow a stationary or posing user to capture the image, but other systems use a real-time algorithm to automatically identify a person’s head and position the object. Significant facial recognition advantages include the fact that it is non-intrusive, hands-free and continuous and approved by most users.

Voice Recognition:

Voice recognition[6] has a tradition going back over four decades, since many analogy filter outputs were measured over time to suit. Voice recognition uses the acoustic characteristics of speech that were found to vary among individuals. Such auditory habits represent both morphology (e.g., throat and mouth size and shape) and learned behavioural (e.g. voice tone, speech style). The integration of trained habits into speech models (the latter named “voiceprints”) has gained speaker identification as a “behavioural biometric” type. Word recognition programs utilize three types of voiced input: text-dependent, text-prompted, and text-independent.

Most speech authentication systems use text-dependent data, in which one or more speech keys are chosen and recorded. Text-prompted feedback is used any time an imposter is involved. The various techniques used to process and store voiceprints include secret Markov models, algorithms matching patterns, neural networks, representation of matrixes and trees for decision taking. Degradation of results may result from adjustments in the voice’s behavioural characteristics and from registration on one phone and checking on another phone. Recognition technologies do need to address speech shifts related to age. Many companies sell speech recognition technologies, mostly as part of major speech synthesis, control and switching schemes. Biometric identification is considered non-invasive. The technology requires little additional hardware by using existing microphones and voice transmission technology which makes long distance recognition through ordinary telephones.

Iris Recognition:

This form of identification utilizes eye iris[7] which is the coloured region around the pupil. Iris variations are considered special. The iris patterns are obtained by an image processing device focused on images. Iris scanning tools have been in usage for many years of use for personal authentication. Iris recognition related systems have declined dramatically in price and this pattern is projected to continue. The system fits well both in modes of authentication and recognition. Even with the case of eyeglasses and contact lenses, real devices may be included. No invasive devices. No physical interaction with a scanner is needed. Iris identification has proved to operate for citizens from various ethnic groups and nationalities.

Hand Geometry:

Such specific authentication mechanisms are well known. For over twenty years hand identification became available[8]. A device may calculate any physical features of the fingertips or of the hands to achieve personal authentication. This involve the weight, width, thickness and hand surface. One fascinating aspect is that a limited biometric sample (few bytes) is needed for some schemes. Hand geometry has achieved recognition in a number of applications. This can also be used in physical access controls in industrial and residential installations, in time and attendance schemes and in general installations for personal authentication.

Signature-Checking:

It technology allows use of a signature's complex[9] analysis for authenticating a individual. The technique is focused on the calculation of the person's velocity, pressure and angle while creating a signature. E-business software and other technologies based on this technology, where signature is an agreed form of personal authentication.

Fingerprint Scanning:

On the hands of a person the shapes of traction ridges and valleys are special to that person. For decades, the law enforcement classifies and establishes identification by matching main ridge ends and bifurcations points. Fingerprints are special to a person's finger even identical twins. One of the most readily accessible biometric technology, mobile fingerprint identification tools and notebook access are now commonly available, consumers don't need to type passwords anymore – now, just a contact gives immediate entry. You may still use the fingerprint systems in authentication mode. Some jurisdictions test signatures on social security applications for prospective claimants to insure the clients don't fraudulently receive benefits with false names. Fingerprints are the ridge and furrow shapes on the palms, which have been used widely to classify people. The biological characteristics of the production of fingerprints are well known, and for decades, fingerprints have been used to classify. Fingerprints have been widely used by the numerous forensic services around the globe since the turn of the 21th century for the detection of suspects. Some citizens feel dissatisfied with using their fingerprints for verification in civilian applications because of their illegal connotations. However, as fingerprint-based biometric systems provide accurate recognition with a very high degree of confidence and lightweight solid-state fingerprint sensors can be installed in different devices (e.g. cell phones), fingerprint-based authentication is becoming increasingly common in a range of civil and commercial applications such as welfare disbursement, mobile phone service. Two major factors in the success of fingerprint-based recognition systems are the development of inexpensive and lightweight solid state scanners, as well as reliable fingerprint matchers. Fingerprints often pose a variety of drawbacks compared with other biometrics.

DESIGN AND WORKING OF BIOMETRIC TECHNIQUE

Design:

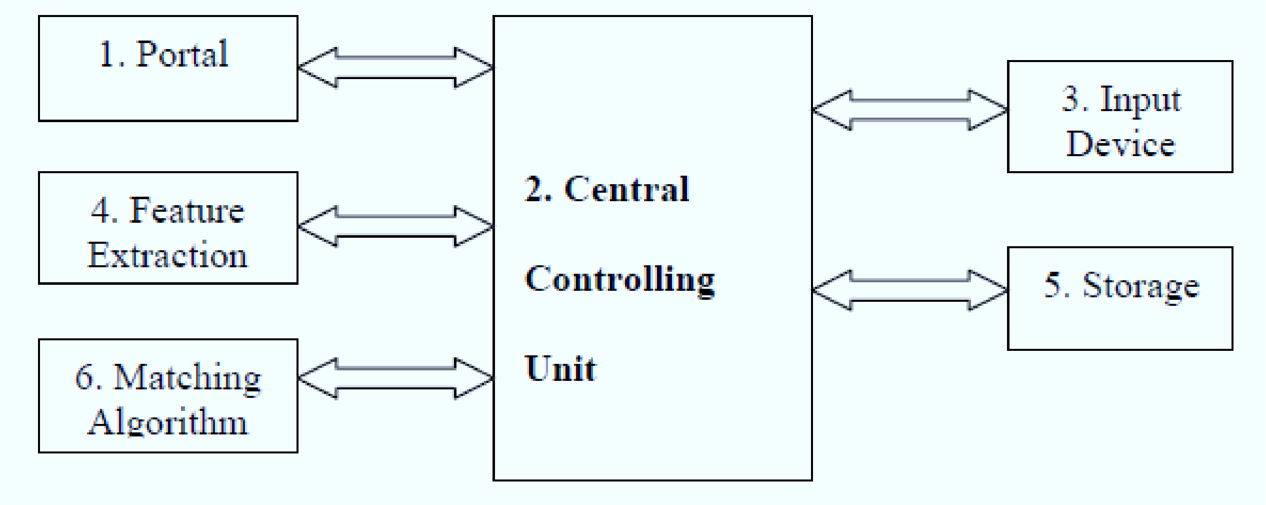

Fig. 1: Block Diagram of Biometric Device

Fig. 1 is show basic block diagram of a biometric system. It contain mainly six component, short description of them is given below.

- *Portal Unit:*

The aim is to protect those properties. The gate at an entry to a building is an illustration of a gateway. If the user has been authenticated successfully, and is allowed to access an item, then permission is given.

- *Controlling Unit:*

It receives the order for authentication, tests the biometric authentication method and returns the app authentication result.

- *Input Unit:*

The input tool is targeted at the acquisition of biometric data. The vivacity and consistency of the sample can be checked by the customer throughout the collection process.

- *Feature extraction Unit:*

The biometric data is processed via this module. The module performance is a collection of derived functions appropriate for the corresponding algorithm. The module can also assess the quality of biometric input data during the feature extraction process.

- *Storage Unit:*

This is biometric prototype data. This is usually going to be more of a folder. Biometric models (e.g. smartcard) may also be placed on a user-held computer. In this case a relation will exist between the consumer and his biometric prototype.

- *Algorithm:*

It contrasts the actual biometric properties to the reference held. The optimal degree of protection threshold may be a corresponding method parameter. In this case the corresponding response will be a yes / no reaction. Then a score is returned reflecting the similitude between the example and the actual biometric sample. And the control machine takes the determination yes / no.

Working:

Biometric technologies operate by capturing the biometric features and analysing them. For certain instances, features are documented as images, but a waveform is reported for speaker recognition, and time series data for signature recognition. Instead of utilizing reported characteristics directly for efficiency purposes, it is common to remove distinguishing features from the samples and encode these features in a manner that enables storage and comparison. When a person first utilizes a biometric device, they enrol their distinguishing features as a guide for potential comparison. Such information may be kept on a central archive, or on a specific computer such as a phone or wallet, depending on the application's needs. Where biometric identification is needed, the biometric characteristics of the person are again registered. However, this time the machine matches the distinguishing features with the recorded relation to assess if there is a near fit.

Biometric detection includes two modes: authentication and description. In authentication, an identification is asserted, and the method of evaluation is restricted to verifying the relation that refers to that identification. No identity claims are required in identification, and the program scans its reference directory to find out if a collected reference matches the recorded biometric properties.

CONCLUSION

This paper show that Biometrics are physical or behavioural features that may be used to distinguish an individual remotely in order to have access to services, computers or records. Since biometrics will offer a fair degree of confidence in authenticating a customer with less hassle, it has the ability to significantly enhance company protection. Computers and devices can automatically unlock when they detect an approved user's fingerprints. Biometrics on fingerprinting is the cheapest, fastest, most convenient and most reliable way of identifying someone. Authentication via fingerprint has several accessibility advantages over standard schemes such as passwords. Based on the performance review, this paper addressed several ideas about privacy and protection of fingerprint biometrics. Future development work on Fingerprint biometrics may be carried out to increase picture accuracy by improving image processing technologies and creating a stronger matching technique for partial and rotated pictures. Based on the study it may conclude that physiological characteristics are more accurate than one that adopts behavioural characteristics, even if the latter might be harder to incorporate in particular applications.

REFERENCES

[1] A. Rice, P. J. Phillips, V. Natu, X. An, and A. J. O'Toole, "Unaware Person Recognition From the Body When Face Identification Fails," *Psychol. Sci.*, 2013, doi: 10.1177/0956797613492986.

[2] C. Hill, "Wearables - The future of biometric technology?," *Biometric Technol. Today*, 2015, doi: 10.1016/S0969-4765(15)30138-7.

[3] F. Blauw and S. Von Solms, "Streamlined approach to online banking authentication in South Africa and Europe," in *2014 IST-Africa Conference and Exhibition, IST-Africa 2014*, 2014, doi: 10.1109/ISTAFRICA.2014.6880608.

[4] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, 2016, doi: 10.1016/j.patrec.2015.12.013.

[5] A. Andics, J. M. McQueen, K. M. Petersson, V. Gál, G. Rudas, and Z. Vidnyánszky, "Neural mechanisms for voice recognition," *Neuroimage*, 2010, doi: 10.1016/j.neuroimage.2010.05.048.

[6] N. Kak, R. Gupta, and S. Mahajan, "Iris Recognition System," *Int. J. Adv. Comput. Sci. Appl.*, 2010, doi: 10.14569/ijacsa.2010.010106.

[7] P. Barré, B. C. Stöver, K. F. Müller, and V. Steinhage, "LeafNet: A computer vision system for automatic plant species identification," *Ecol. Inform.*, 2017, doi: 10.1016/j.ecoinf.2017.05.005.

[8] S. K. Garg, S. Versteeg, R. Buyya, R. Jain, M. Faisal, and Y. Chen, "Signature redacted Signature redacted Signature redacted Signature redacted," *Proc. - 2011 4th IEEE Int. Conf. Util. Cloud Comput. UCC 2011*, 2014, doi: 10.1109/UCC.2011.36.

[9] I. B. Durowoju, K. S. Bhandal, J. Hu, B. Carpick, and M. Kirkitadze, "Differential scanning calorimetry — A method for assessing the thermal stability and conformation of protein antigen," *J. Vis. Exp.*, 2017, doi: 10.3791/55262.