IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 8, August 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Biometric Authentication Technologies and Applications

Benedict Mbanefo Emewu [1], **Vincent O.C** Eke[2]

[1] Computer Science Department, Ebonyi State University,
Abakaliki, Ebonyi State, Nigeria.

[2] Computer Science Department, Ebonyi State University,
Abakaliki, Ebonyi State, Nigeria.

Abstract

Human beings use natural abilities to recognize an individual through their face, voice, gait and other characteristics. Whereas, computers require programming algorithms in order to recognize an individual using the same observable information. Technological advances are promising to close the gap between human perception and computer recognition. Biometrics is seen by many as a solution to a lot of the user identification and security problems. This paper presents an overview of the biometrics authentication technology, its utilization and introduces the resent issues underlying the biometrics. Biometric recognition refers to the automatic recognition of individuals based on their physiological and or behavioral characteristics. By using biometrics it is possible to confirm or establish an individual's identity based on "who she is", rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password).

Keywords: *Biometrics, Distinctiveness, Facial Imaging, Fingerprint, Iris Recognition, Speaker Verification.*

.

1. Introduction

Humans have used characteristic such as face, voice, gait, etc for thousands of years to recognize each other. Any two persons should be sufficiently different in terms of the characteristic, in clear term 'Distinctiveness'.

The term biometrics is derived from the Greek words bio meaning "life" and metrics meaning "to measure". For our use, biometrics refers to technologies for measuring and analysing a person's physiological or behavioural characteristics. These characteristics are unique to individuals hence can be used to verify or identify a person. Biometrics refers to the identification or verification of a person based on his/her physiological and/or behavioural characteristics.

Several verification/identification based biometrics have evolved based on various unique aspects of human body, ease of acquiring the biometric, public acceptance and the degree of security required. This paper presents an overview of various biometrics in use/proposed and their applicability to different activities

Biometrics relies on measuring a variety of anatomical, physiological and behavioural characteristics and matching to measurements that were previously collected from the person, thus recognizing the person using distinctive personal traits such as fingerprint, face, voice and so forth. For instance, fingerprint based recognition system; the person must place his finger on a fingerprint sensor whenever he wants to log in. The sensor will capture the fingerprint image he provides and will then match it to previously collected fingerprint measurements. If the latest fingerprint measurement matches closely enough, the system acknowledges that the genuine person is present and logs him in or grants him access. It is worth noting that the person has no device to lose or password to forget: he can authenticate himself as long as his fingerprint (biometrics characteristics) hasn't been badly injured or degraded. Biometrics thus can provide one of the most substantial benefits to the security arena in guarding against attempts to establish fraudulent multiple identities or prevent identity fraud. As, biometrics cannot be shared due to being an intrinsic property of an individual, therefore making it possible to know automatically who did 'what', 'where' and 'when'. Anyway, the principal goal of the use of biometrics is to attain the capability of accurately recognizing individuals with greater reliability, convenience, speed and lower cost, [1].

Depending on the context, a biometric system can be used either in a verification mode or an identification mode. In verification (Am I who I claim I am?) mode, a person's claimed identity is confirmed based upon validating a sample collected against a previously collected biometric sample for that individual. On the other hand, in identification (Am I who I claim I am? or Who am I?) mode, the system has to recognize a person based upon comparison of biometrics collected against a database of previously collected samples of N individuals, [2].

1.2 Why Biometrics

While it is possible to copy or mimic some biometric traits, it is generally more difficult to produce such a trait and present it to a supervised sensor than to share a password or token. If the system is unsupervised, an attacker may not need to spoof the trait physically; he might have a copy of the bit string or the reference, which would make such an attack no more difficult than compromising other forms of recognition.

More precisely, biometric authentication is a binary hypothesis test where the hypothesis is that the biometric sample input matches to a degree of certainty the claimed biometric reference enrolment. The overall system then uses the matching results to accept or reject this hypothesis, [3].

2 Literature Review

More accurately, fingerprints represent the transition from a manual biometric to the automated form of the technology. Fingerprints have long been used to identify people. In 14th century China, they were used as a form of signature. Today, fingerprint verification technology is the most prominent biometric technology, used by millions of people worldwide. It is estimated that the number of possible fingerprint patterns is 10 to the 48th power. Fingerprint technology can be used effectively in both verification (1:1) and identification (1:N) applications, [4].

2.1 Biometric Security

Biometric security could play an important role in securing future computer systems. Biometric devices could create a more ambiguous and user friendly environment for its users. Lost or stolen cards and passwords can cause major headaches for support desks and its users. This problem is irradiated in biometric security since it is practically impossible for a user to forget or leave their hand or eye at home. Also other forms of identification methods which rely on the user remembering a password or a user carrying an object such as a smart card are easier to compromise compared to biometrics. For example approximately 25% of ATM card users write the PIN on their ATM card thus making the PIN security useless, [5]. Since biometric devices measure unique characteristic of each person, they are more reliable in allowing access to intended people. Resources can then be diverted into other uses, since they are not being wasted on the policing of purchased tickets or resetting passwords.

Imagine a scenario where you are your own key to everything. Your thumb opens your safe, starts your car and enables access to your account records. This could seem very convenient. However once biometric security is attacked you can’t exactly change what your finger print or change your DNA structure. And since your biometric data is not a secret as such, as you touch objects all day and your iris scan can be collected from anywhere you look. A large security risk is created if someone steals your biometric information as it remains stolen for life. Unlike conventional authentication methods you cannot simply ask for a new one, [6].

Biometrics could become very useful but unless handled properly are not to be used as keys, as keys need to be secret, have ability to be destroyed and renewed, at the present stage biometrics do not have these qualities. Although still in its primitive stages a proposal for biometric authentication based on cryptosystem keys containing biometric data by Yukio itakura and Shigeo Tsujii enables biometric devices to be secure and more reliable when used as a key. This system works by generating a public key from two secret keys, one generated from the hash function of the biometric template data another secret key is created from a random number generator, [7].

3 Biometric Systems

3.1 Basic Structures

A generic biometric system consists of five main modules: a sensor module; a quality assessment and feature extraction module; a matching module; Decision making module; a system database module, as described below.

1. Sensor module: A suitable biometric sensor/scanner is applied to attain the raw biometric data of an individual. For instance, an optical sensor can be used to acquire the fingerprint images by capturing the friction ridge structure of the finger. Since, sensor module determines the interaction of the human with the system, thus playing a pivotal role in the performance of the biometric systems.
2. Quality assessment and feature extraction module: A quality assessment algorithm is used, in order to determine the suitability of the biometric data for the subsequent processing. If the quality is inadequate then the biometric sample is rejected and reacquired. If the quality assessment algorithm is not incorporated then the acquired data is subject to signal enhancement algorithm to improve its quality. The biometric sample is then processed to glean a set of salient discriminatory features. The extracted feature set procured during enrolment is stored in the database, referred as template, thereby constituting the identity of an individual.
3. Matching module: To verify the identity of an individual, the extracted feature set from the biometric sample (known as query or input or probe) is compared against the enrolled template to generate the match score, which determines the amount of similarity (similarity score) or distance (distance

score) between the two feature sets. The system conducts a one-to-one comparison to verify a claimed identity, while the comparison is one-to-many to determine an identity.

4. Decision making module: Decision making module uses match score, to validate a claimed identity in the verification task or to provide a ranking of the enrolled identities to identify an individual in the identification task. In order to determine the authenticity of an individual, generally, the match score is compared to a predefined threshold. The identity of an individual is verified successfully, if the match score of the query is equal or higher than the threshold for “similarity score”, while equal or lower for “distance score”.
5. System database module: The system database, which acts as the depository of biometric information, is used to store the extracted feature set from the raw biometric sample (i.e., template), along with some biographic information (such as name, Personal Identification Number (PIN), address, etc.) characterizing an individual.

3.2 Enabling Technology

The enabling technologies in biometric authentication technology measures and analyze human biological and behavioral characteristics. Identifying a person’s biological characteristics is based on direct measurement of a part of the body, such as speaker recognition, facial features, fingerprints and iris patterns will be looking at the general principles or how a particular technology or product works.

3.2.1 Speaker Verification

Fig. 1 Speaker verification

How the Technology Works: Speaker verification has strong behavioral and biological components as shown in fig. 1. The differences in how people’s voices actually sound can result from a combination of biological differences, such as the shape of the vocal tracts, and from individual speaking habits. Speaker verification technology uses these differences to create a voice print template that can be used to verify the identity of a person by comparing the unique patterns generated as a result of these differences. Speaker verification is separate and distinct from “voice recognition,” which is the recognition of spoken words and typically used in automated telephone directory services and in dictation systems. Unlike speaker verification, voice recognition is not a biometric technology since it does not confirm individual identity. Speaker verification has traditionally focused on the sound of the voice that is generated by the resonance in the vocal tract. The length of the vocal tract and the shape of the mouth and nasal cavities affect the voice. Speaker verification is defined as “the automated process of identifying a specific individual’s voice.” Typically during enrolment, the speaker verification system will capture samples of a person’s voice by having him/her repeat a set of pre-determined words, sentences, or phrases into a microphone or telephone. As with other biometrics, an enrolment template is generated and stored for future comparisons. This template is often referred to as a “voice print.” Speaker verification systems can be of two types: text independent or text-dependent. Text-dependent systems, during enrolment, capture samples of a person’s voice by having him/her repeat a set of pre-determined words, sentences, or phrases into a microphone or telephone. This technique enhances the verification (and in some limited use, recognition) but requires a cooperative and patient user. In text-independent recognition, however, the user does not have to say a pre-determined phrase nor cooperate or even be aware of the recognition system. Consequently, text-independent recognition has been used when trying to identify or recognize a speaker from radio or telephone signals.

Advantages: There are many advantages to using speaker verification. It provides eye-and hands-free operation, is reliable, flexible, and has a good data accuracy rate.

Disadvantages: Different people can have similar voices and a person’s voice can vary over time due to changes in health, emotional state, and age. Physical conditions of the voice, such as those due to sickness, can affect the speaker verification process, and since changes are likely to occur with age, waiting long periods between comparisons could affect long-term accuracy. Speaker recognition models are typically large, often on the order of 6Kb per speaker.

Applications: Text-dependent speaker verification systems have been used in logical access control applications and where remote identity verification is required. A major example of this is call centre automation, where transaction processing is automated via telephone or computer. Popular uses include financial transactions and credit card processing (address changes, balance transfers, loss prevention). Speaker verification/recognition has also made an impact in the penal system where it is used to monitor and control inmate phone privileges and identity verification of parolees, juvenile inmates, and those under house arrest.

3.2.2 Facial Imaging or Recognition

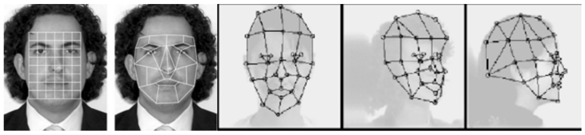

Fig. 2 Facial imaging

How the Technology Works: Facial imaging or recognition identifies people by comparison of sample images to stored templates using mathematical analysis of the groups of acquired pixels. Facial imaging is not based on common "facial features," such as cheeks, nose, chin, and mouth, which cannot be found reliably by current algorithms. Most systems, however, must find the eye centres for the purpose of isolating the face in a large image. Systems using facial recognition technology capture facial images using digital cameras and, like their biometric technology counterparts, generate templates for comparing a live face to a stored enrolment template. Facial recognition is most commonly used in the verification mode.

Advantages: The concept of recognizing someone by his/her face is intuitive and the most common means humans use to identify one another on sight. Because of this, there are several advantages to using facial recognition, including:

- Facial recognition can leverage existing databases that currently house facial images or photographs.
- Facial images can be captured from some distance away, providing a clandestine or covert capability, if needed. Hence perceived as the only biometric suitable for "surveillance" applications and many more application.

Disadvantages: The majority of facial recognition algorithms seem to be sensitive to variations in Pose angle, Illumination, facial Expression, and Currency.

Applications: With facial recognition, performance can be greatly influenced by the type of application setting that is used. Application environments for facial recognition systems can be categorized as "controlled" and "random." Facial recognition, with heavy operator assistance and not in the automatic mode, has been used to identify card counters in casinos. Facial recognition has also been successful in access control, whether to a location, building, room, or for computer access. Face recognition has been successfully applied as a tool for screening individuals to see if they are already known to the system. This is used for fraud prevention when individuals apply for visas or driver's licenses. The same technique is used in some law enforcement jurisdictions during the criminal booking process to get an immediate indication of the identity of an arrestee well before a FBI fingerprint check is conducted. This technology can be overt or covert in nature.

3.2.3 Fingerprint

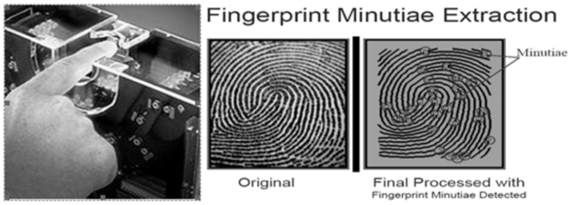
Fingerprint Minutiae Extraction
Minutiae
Original
Final Processed with
Fingerprint Minutiae Detected

Fig.3 Fingerprint extraction

How the Technology Works: Fingerprint verification systems work by identifying the locations of small lines or ridges found in the fingerprint. They extract features from impressions that are made by these distinct ridges. Typically, fingerprints are either flat (capture by placing a finger directly on the scanner) or rolled (rolling the finger from one edge of the fingernail to the other). A flat fingerprint is an impression of the area between the fingertip and the first knuckle, which a rolled fingerprint also include as an impression of the ridges on both sides of the finger. Fingerprint-based systems can also be further categorized into four broad groups: Minutiae-based matching (analysing the local structure), direct correlation techniques, optical comparison, and spectral ridge-pattern matching (analysing the ridge or global structure) of the fingerprint. When fingerprint patterns are captured and analysed, about 5% of all fingerprint patterns are arches; 30% are whorls; and 65% are loops, divided approximately equally into left and right loops.

In matching ridge patterns, the image is divided into small square areas about five pixels on a side. The ridge wavelength, direction, and phase displacement for each small square is encoded and used as the basis for the biometric template. Ridge pattern matching algorithms use a process of aligning and overlaying segments of fingerprint images to determine similarity.

Minutia-based Algorithms a typical fingerprint image may produce between 15 and 70 minutiae, depending on the portion of the image captured. The most prevalent minutiae are ridge endings. Minutiae algorithms plot the relative position and type of points (minutiae) where ridge lines branch apart (bifurcate) or terminate (end).

Advantages: Fingerprint patterns are stable throughout one's lifetime, and unique and easily analysed and compared. Fingerprint systems are easy to use, in most cases requiring the user to simply touch a platen with his/her forefinger. In addition to being secure, most fingerprint systems are relatively inexpensive.

Disadvantages: Capable of high accuracy levels, fingerprint devices can suffer from usage errors when users are not properly trained in system usage and/or motivated to cooperate when placing their finger(s) on the reader. This is, of course, not limited to fingerprint systems and extends to all biometric technologies. Conditions must be right for accurate authentication; for example, wet or moist fingers, cuts on fingers, or dirt or grease can sometimes affect the authentication process. Additionally, as with other biometric methods where a platen must be touched, some people are uncomfortable with touching something that other people have touched repeatedly before them. Other concerns involve the aspects of occupational impact. The use of hands in constant contact with abrasives or chemicals may interfere with fingerprint readers. There are consistent reports of genetic influence in population segments regarding an impact on image quality, but good documentation on this "outlier" influence is hard to find.

Applications: Fingerprint biometrics have four main application areas: large-scale Automated Fingerprint Imaging Systems (AFIS) that are generally used by law enforcement, for fraud prevention in entitlement programs, physical access control (doors) and "logical" access to computer systems. Workstation access applications seem to be based almost exclusively around fingerprints, due to the relatively low cost, small size (easily integrated into keyboards, mice, and laptops) and ease of integration.

3.2.4 Iris Recognition

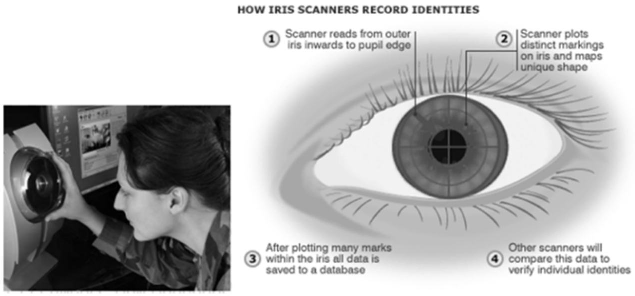
HOW IRIS SCANNERS RECORD IDENTITIES
1 Scanner reads from outer iris inwards to pupil edge
2 Scanner plots distinct markings on iris and maps unique shape
3 After plotting many marks within the iris all data is saved to a database
4 Other scanners will compare this data to verify individual identities

Fig. 4 Iris Scanning

How the Technology Works: Iris recognition technology is based on the patterns resident in the iris of the eye (i.e. the colour ring surrounding the pupil) Iris recognition technology identifies people by the unique patterns in the iris using a fairly conventional charge coupled device (CCD) camera. Made from elastic connective tissue, the iris represents a richly patterned surface under the reflective cornea of the eye. The image of the iris under infra-red illumination can be quantified and used to identify an individual. Approximately 2048 binary (0 or 1) features are captured in a "live" iris identification application. Formed by the eighth month of gestation, iris characteristics reportedly remain stable throughout a person's lifetime, except in cases of trauma or injury. Iris recognition systems use a CCD camera to capture a black-and-white, high-resolution image of the iris under infra-red illumination. They then define the boundaries of the iris, establish a coordinate system, and define the "zones for analysis." All parts of the visible iris are processed into a reference (template) that is often referred to as an IrisCode. The software locates and "eliminates" (does not encode) data from eyelashes, eyelids and other "non-iris" sources (e.g., light reflections). Algorithms check for a specific pattern reflected on the eye and may use additional measurements to determine that the eye is living. The visible characteristics within the "zones of analysis" are converted into a 512-byte template that is used to identify the individual; 256 of these bytes are control code. Most physical access control applications require a person to stand within three to 10 inches of the camera and look directly into the lens, centering his/her eye based on guidance light or illuminated pattern on a two-way mirror in front of the user. More interactive systems may "verbally" prompt or signal the user to adjust his/her distance for proper image capture. Some systems using desktop or hand-held cameras can operate at a distance of about 12 to 18 inches.

Advantages: It can take one to two seconds for an iris recognition system to identify a person's iris pattern. A template iris pattern code (or IrisCode) contains less than half of a kilobyte of data, resulting in a small "electronic footprint." Up to one million records-per-second can be scanned using a standard personal computer. Iris-based systems have the lowest false match rates among all currently available biometric methods, and are the least intrusive technique of the eye-based biometrics. It is one of the few biometric systems, besides fingerprinting, that works well in "identification" (one-to-many comparison) mode.

Disadvantages: Ease of use can be an issue with some iris recognition based systems since the user must line-up his/her eye with the camera. In most cases, the current technology does not lend itself to surveillance applications or where users are moving quickly, as it requires the user to stop for a few seconds and look directly into the camera to be identified. Most people believe that the imaging of their irises will reveal their medical conditions and diseases, such as pregnancy, heart disease, diabetes, AIDS, or high blood pressure. No scientific study has established that iris recognition templates can provide information about a person's health, and iridology has no known scientific support.

Applications: Some programs and applications include: Airline passenger screening, border security, facility access control, computer login, ATMs, inmate identification in correctional facilities, and grocery stores (for automated check-out).

CONCLUSION

Conventional authentication technologies are not able to provide the necessary assurance about who you are and are not capable of protecting against the virulent attacks that are targeting both users and business. Biometrics does offer the possibility to provide additional assurance, but Continuous Authentication is required if this to be effective. In spite of all the claims, not all biometric technologies are suitable and organizations should ask a number of key questions before implementing solutions.

REFERENCES

[1] A. Zahid., (2012), "Basic Structure of A Biometric System", Security Of Multimodal Biometric Systems Against Spoof Attacks, University Of Cagliari, Cagliari, Pp 12-13.

[2] N.P Joseph and I M Lynette., (2010), "Fundamentals of Biometric Recognition And Human Individual Distinctiveness", Biometric Recognition: Challenges And Opportunities, National Research Council, Washington D.C, Pp 3

[3] J. Smith, (2015), "The Way Forward", Future of Biometric Authentication Technologies, Techcrew, Chicago, Pp 47.

[4] S. Marios, (2003), "What Are Biometrics?", Introduction To Biometric Recognition Technologies And Applications, Carnegie Mellon Cylab, Pittsburgh, 5th Edition, Pp 2

[5] J.L. Dunker, (2004), "Biometric Limitations", Fundamentals of Biometric Authentication Technologies, NY-Biotech, New York, Pp 16.

[6] M. Schneier, (1999), "Biometrics", Security Of Multimodal Biometric systems Against Spoof Attacks, University Of Cagliari, Cagliari, Pp 5-7

[7] T. Behaviosec, (2011), "Biometric Myths", The Role Of Biometrics In IT Security And Continuous Authentication, Behaviometrics AB, Pp 6-7