A Survey of Emerging Biometric Technologies

Olufemi Sunday Adeoye
Department of Computer Science
University of Uyo

ABSTRACT
Computer Security System / technology have passed through several changes. The trends have been from what you know (e.g. password, PIN, etc) to what you have (ATM card, Driving License, etc) and presently to who you are (Biometry) or combinations of two or more of the trios. This technology (biometry) has come to solve the problems identified with knowledge-based and token-based authentication systems. It is possible to forget your password and what you have can as well be stolen. The security of determining who you are is referred to as BIOMETRIC. Biometric, in a nutshell, is the use of your body as password. This paper explores the various methods of biometric identification that have evolved over the years and the features used for each modality.

Keywords: Biometrics, minutiae, verification, distinctiveness, measurable, features

1.0 INTRODUCTION
Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity. Automated use means using computers or machines, rather than human beings, to verify or determine physiological or behavioral characteristics. Physiological or behavioral characteristics are distinctive, which provide basic measurement of biometrics.

Physiological biometrics are based on direct measurements of a part of the human body, such as finger-scan, facial scan, iris-scan, hand-scan, and retina-scan.

Behavioral biometrics are based on measurements and data derived from an action and therefore indirectly measure characteristics of the human body, such as voice-scan and signature-scan. The element of time is essential to behavioral biometrics because it may change with time.

A biometric can also be defined as any measurable, robust, distinctive physical characteristic or personal trait that can be used to identify, or verify the claimed identity of, an individual. Biometric authentication refers to automated methods of identifying, or verifying the identity of, a living person.

Measurable means that the characteristic or trait can be easily presented to a sensor and converted into a quantifiable, digital format. This allows for the automated matching process to occur in a matter of seconds.

The robustness of a biometric is a measure of the extent to which the characteristic or trait is subject to significant changes over time. These changes can occur as a result of age, injury, illness, occupational use, or chemical exposure. A highly robust biometric does not change significantly over time. A less robust biometric does. For example, the iris, which changes very little over a person's lifetime, is more robust than a voice.

Distinctiveness is a measure of the variations or differences in the biometric pattern among the general population. The higher the degree of distinctiveness, the more unique the identifier. The highest degree of distinctiveness implies a unique identifier. A low degree of distinctiveness indicates a biometric pattern found frequently in the general population. The iris and the retina have higher degrees of distinctiveness than hand or finger geometry. The application helps determine the degree of robustness and distinctiveness required.

Living person distinguishes biometric authentication from forensics, which does not involve real-time identification of a living individual.

2. DISCUSSION
2.1 Emerging Biometric Modalities
Different types of biometric technologies focus on different physical characteristics. Within the biometric community, these different applications are referred to as "modalities". The emerging biometric modalities include: Hand, Face, Fingerprint, Gait, Signature, Voice, Iris, Retina, Vein, DNA, Body Odor, Ear Pattern, Keystroke and Lip. Generally, biometric modalities can be categorized into four types: Hands, Heads and Face, Other Physical Characteristics and Behavioral Characteristics.

2.1.1 Hand Geometry
Hand geometry systems are currently among the most widely used biometric technologies. Biometric hand recognition systems measure and analyze the overall structure, shape and proportions of the hand, e.g. length, width and thickness of the hand, fingers and joints, characteristics of the skin surface area such as creases and ridges.

As hand biometrics rely on hand and finger geometry, the system will also work with dirty hands. The only limitation is for people with severe arthristis who cannot spread their hands on the reader.

The user places the palm of his/her hand on the reader's surface and aligns his or her hand with the guidance pegs which indicate the proper location of the fingers. The device checks its database for identification and verification of the user. The process normally takes a few seconds.

To enroll, the user places his/her palm down on the reader's surface. The image acquisition system comprises of a light source, a camera, a simple mirror and a flat surface (with five pegs on it). The user places his hand-palm facing downwards-on the flat surface of the device. The five pegs serve as control points for an appropriate placement of the right hand of the user. The device also has knobs to change the intensity of the light source and the focal length of the camera. The lone mirror projects the side-view of the user's hand onto the camera. The device is hooked to PC with a GUI application which provides a live visual feedback of the

top-view of the hand. The GUI aids in capturing the hand image.

Feature extraction involves computing the widths and lengths of the fingers of various locations using the captured image. These metrics define the feature vector of the user's hand. To prevent a mold or a cast of the hand from being used, some hand biometric systems will require the user to move their fingers. Also, hand thermograph can be used to record the heat of the hand, or skin conductivity can be measured.

An individual's hand does not significantly change after a certain age. Individual hand features are not descriptive enough for identification. However, hand biometric recognition systems are accurate for verification purposes when combining various individual features and measurement of fingers and hands (Arum Ross and Anil Jain). Hand biometric is beneficial because it is easy to use, non intrusive and require small amount of data to uniquely identify a user. With this a large number of templates can be easily stored in a standalone device. The weaknesses of this biometric are lack of accuracy, size of the scanner fairly expensive, compared with fingerprint systems and injuries to hands can prevent the hand biometric system from working properly. Hand biometrics are currently used in gaining access to restricted areas and building and in taking record of attendance and time employee reported for work.

2.2 Face Biometrics

Face recognition can be an import alternative for selecting and developing an optimal biometric system. Its advantage is that it does not require physical contact with an image capture device (camera). A face identification system does not require any advanced hardware, as it can be used with existing image capture devices (webcams, security cameras, etc). Thus, facial recognition should be considered as a serious alternative in the development of biometric or multimodal systems (multi-biometric systems).

Facial recognition technology is a widely used biometric system. Usually these systems extract certain features from face images and then perform face matching using these features. Specific features of a face include the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin and so forth. A face does not have as many uniquely measurable features as fingerprint and eye irises. So facial recognition reliability is slightly lower than these other biometric recognition methods. However, it is still suitable for many applications, especially when taking into account its convenience for user. Facial recognition can also be used together with fingerprint recognition (as we now have in most laptop/notebook computer) or another biometric method for developing more security-critical applications.

The multi-biometric approach is especially important for identification (one-to-many) systems. In general, these identification systems are very convenient to use because they do not require any additional security information (smart cards, passwords, etc). However, using one-to-many matching routines with only one biometric method can result in a higher false acceptance with large database. Using face identification as an additional biometric method can dramatically decrease this effect. This multi-biometric approach also helps in situations where a certain biometric feature is not optimal for certain groups of users. For example, people who do heavy labour with their hands may have rough fingerprints, which can increase the false rejection rate if fingerprint identification was used alone.

2.3 Gait Biometrics

A unique advantage of gait as a biometric is that it offers potential for recognition at distance or at low resolution, when other biometrics might not be perceivable [14].

Recognition can be based on the (static) human shape as well as on movement, suggesting a richer recognition cue. Further, gait can be used when other biometrics are obscured-criminal intent might motivate concealment of the face, but it is difficult to conceal and/or disguise motion as this generally impedes movement.

Early medical studies revealed many of the basic tenets of gait analysis [12]. The biomechanics' literature makes similar observations "A given person will perform his or her walking pattern in a fairly repeatable and characteristic way, sufficiently unique that it is possible to recognize a person at a distance by their gait" [20].

2.4 Iris Biometrics

Iris recognition is a biometric identification technology that uses high- resolution images of the rides of the eye. The iris of the eye is well suited for authentication purposes. It is an internal organ protected from most damage and wear, it is practically flat and uniform under most conditions and it has a textile that is unique even to genetically identical twins [2].

The first step in iris recognition is to locate the iris using landmark features. These landmark features and the distinct shape of the iris itself allow for imaging, feature isolation, and image extraction. To obtain a good image of the iris, recognition systems typically illuminates of the iris with near-infrared light, which can be observed by most cameras but is not detectable by, nor can it cause injury to, humans. Images of the iris are used to generate a template, a set of data that maps the patterns of the iris and the location on the iris where the patterns exist [15, 16].

Iris recognition algorithms produce remarkable results. Daugman's algorithms have produced accuracy rates in authentication that are better than those of any other method. Iris code, a commercial system derived from Daugman's work, has been used in the United Arab Emirates as a part of their immigration process. After more than 200 billion comparisons, there has never been a false match [6].

2.5 Voice Biometrics

Voice biometrics, also known as "speaker recognition", is a biometric modality that uses an individual's voice for verification and/or identification. Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style, tone, cadence and frequency of a person's voice). This incorporation of learned patterns into the voice templates (the latter called "Voiceprints") has earned speaker recognition its classification as a "behavioral biometric." Voice biometrics systems employ three styles of spoken input: text-dependent, text-prompted and text-independent. Most speaker verification applications use text-dependent input, which involves selection and enrollment of one or more voice passwords. Text-prompted input is used whenever there is concern of imposters. The various technologies used to process and store voiceprints include hidden marker models, pattern matching algorithms, neural network, matrix representation and decision trees. Some systems also use "anti-speaker" techniques, such as cohort models, and world models [17].

2.6 Signature Biometrics

This technology uses the dynamic analysis of a signature to authenticate a person. Dynamic signature measures the speed and pressure an individual uses when signing his or her name-not what the signature itself looks like [15, 16]. It is based on measuring speed, pressure and angle used by the person when a signature is produced. Common dynamic characteristics include the velocity, acceleration, timing, pressure, and direction of the signature strokes-all analyzed along the X, Y, and Z axes. These characteristics are collected using contract-sensitive technologies such as Personal Digital Assistants (PDAs) or digitizing tablets [10]. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication.

2.7 Fingerprint Biometrics

Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available from many different vendors at a low cost. With these devices, users no longer need to type passwords-instead, only a touch provides instant access. Fingerprint systems can also be used in identification mode [9].The biometric fingerprint sensor takes a digital picture of a fingerprint. The fingerprint scan detects the ridges and valleys of a fingerprint and converts them into ones and zeroes. Complex algorithms analyze this raw biometric scan to identify characteristics of the fingerprint, known as the "minutiae". Minutiae are stored in a template, but only a subset of these has to match for identification or verification. In most systems, if 10 to 20 minutiae match, the fingerprint is considered a match. In today's smart card systems approximately 40 minutiae are stored, because of space restrictions.

2.8 Retina Biometrics

The retina, the layer of blood vessels situated at the back of the eye, forms a unique pattern. Retina biometrics are generally regarded as the most secure biometric method [4]. Retina scanners compare the blood vessels in the eye. A scanning device that uses low light compares unique patterns on the retina. The presence of glasses adversely affects retina scanning.

A retina scan produces at least the same volume of data as a fingerprint image. In practice, the retina scanning is used mostly for verification. The size of the eye signature template is 96 bytes. Retina scanning is used only rarely today because it is not user friendly and still remains very expensive. Retina scan is suitable for application where the high security is required and the user's acceptance is not a major aspect [21].

2.9 Vein Biometrics

Vein patterns on the eye's retina are known as one of the most unique characteristics owned by humans. This pattern is not genetically determined, but is randomly developed by each individual. It is one of the most stable characteristics in the life of a person [7]. The vein structure, or "vein tree", is captured using infrared light.

2.10 DNA Biometrics

DNA (deoxyribonucleic acid) is the well-known double helix structure present in every human cell. A DNA sample is used to produce either DNA fingerprint or a DNA profile. The current processes for obtaining DNA samples are quite intrusive, requiring some from of tissue, blood or other bodily sample. DNA testing is a technique with a very high degree of accuracy. The statistical sampling shows a 1-in-6 billon chance of two people having the same profile. It is the most distinct biometric identifier available for human beings except for monozygotic twins. DNA does not change throughout a person's life; therefore its permanence is incontestable. It is currently used in forensics and paternity tests.

2.11 Body Odor Biometrics

Body odor recognition is a contactless physical biometric that attempts to confirm a person's identity by analyzing the olfactory properties of the human body scent. According to the University of Cambridge the sensors that have been developed are capable of capturing the body scent from non-intrusive body parts, such as the hand [8]. Each chemical of the human scent is extracted by the biometric system and converted into a unique data string.

2.12 Ear Pattern Biometrics

The shape of the outer ear, lobes, bone structure and the size are unique to each person. Ear pattern recognition is employed as a physical contactless biometric and uses an optophone to verify the shape of the ear [3].

A French company, ART Techniques, developed the optophone and the process. It is a telephone type handset, which is comprised of two components (lighting source and cameras). Much like the minutiae points of a palm print or fingerprint the outer ear has many detailed features that can be measured and compared to a biometric template.

2.13 Keystroke Dynamics

Keystroke dynamics is an automated method of examining an individual's keystrokes on a keyboard. The technology uses a keyboard compatible with PCs. This technology examines such dynamics as speed and pressure, total time of typing a particular password, and the time a user takes between hitting certain keys. Keystroke dynamics has the potential for continuous authentication of identity while a person is using a computer [1].

2.14 Lip Biometrics

Lip prints are the normal lines and fissures in the form of wrinkles and grooves present in the zone of transition of human lip, between the inner labial mucosa and outer skin. This structure is not given by any anatomical name [20]. The appearance of lip prints look like finger prints and vary from individual to individual.

If a definite and detail description of the different parts of upper lip and lower lip are established for an individual by detailed study made as an anti mortem record, this anti mortem record can be used for matching the details of lip prints recorded in an unknown deceased person in post mortem records for personal identification. In comparing the lip print of anti mortem record and post mortem record, if both the lip prints are matched, the individual can be identified. The basic features in lip print are furrows on the red part of the human lip, lip grooves, labial wrinkles and color of rouge.

3 KEY ELEMENTS OF ALL BIOMETRIC SYSTEMS

All biometric systems consist of three basic elements which are Enrollment, Templates, and Matching.

3.1 Enrollment

Enrollment is the process of collecting biometric samples from a person and the subsequent generation of a template. Typically, the device takes three samples of the same biometric and then averages them to produce an enrollment template.

3.2 Templates

These are the data representing the enrollee's biometric. They are created by the biometric device, which uses appropriate algorithm to extract features appropriate to that technology from the enrollee's samples. These features are also referred to as minutiae points for some technologies, such as fingerprint systems. Because templates are only a record of distinguishing features of a person's biometric characteristic or trait, (and not an image or complete record of the actual fingerprint or voice), the template is usually small and allows for the near – instantaneous processing time characteristic of biometric authentication. The small size of some templates allows for storage on magnetic stripes or bar codes placed on plastic cards or smart cards.

3.3 Matching

Matching is the process of comparing submitted biometric sample against one (verification) or many (identification) templates in the system's database. There are three ways a match can fail: failure to enroll, false match, and false non match. Failure to enroll (or acquire) is the failure of the technology to extract distinguishing features appropriate to that technology. Two reasons account for this failure: the individual's fingerprints are not distinctive enough to be picked up by the system, or the distinguishing characteristics of the individual's fingerprints have been altered because of the individual's age or occupation, e.g. an elderly bricklayer.

Besides, the possibility of a false match or a false non match exists. These two terms are frequently misnomered "false acceptance" and "false rejection", respectively, but these terms are application – dependent in meaning. A false match occurs when a sample is incorrectly matched to a template in the database (i. e., an imposter is accepted). A false non match occurs when a sample is incorrectly not matched to a truly matching template in the database [1].

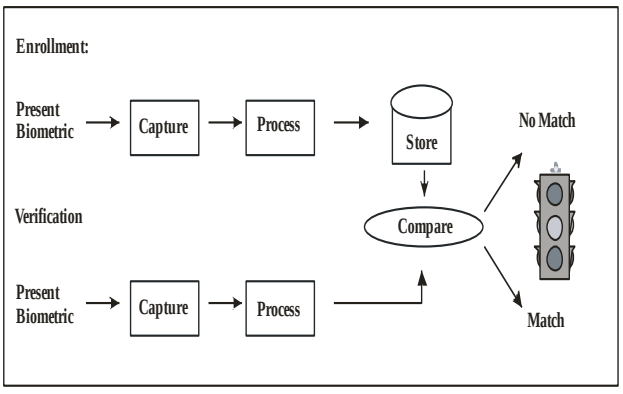

Fig.1 Typical Biometric Enrolment and Matching Process.

4.0 CONCLUSION

Biometrics is an emerging and ever changing field of technology that can be implemented into just about anything that requires a security protocol. While the cost of implementation is high the benefits of increased security, peace of mind, lessening of man hours, and of course the increase of accessibility by people of variable abilities may justify the cost.

Indeed, the reliance on the latest technology may make a company even more vulnerable by creating the illusion of security. This is why governmental agencies and commercial companies must remain eternally vigilant and continually seek out the most up-to-date method of securing the technological assets of an enterprise.

5.0 RECOMMENDATIONS AND NEXT STEP

Biometric technology has come to stay. It is the technology of the millennium. Since its inception, it has been used in various areas where security is very crucial. Since biometrics can be implemented by companies, governments, customs, churches hospitals banks and military (police, army, navy, air force) to verify peoples identity, I hereby recommend its use in the commercial, production and end-user environment. With the continuous use of this technology the future is already in the palm of our hands.

Moreover, going by the event of 9/11 in America, it simply suggest that biometric should be part of any country's security program.

6.0 REFERENCES

[1] Army Biometric Applications. www.biteproject.org/documents/rand-report-biometric.pdf.

[2] Biometric Consortium Web Site: http://www.Biometric.org

[3] Carreira-Perpinan (1995), Ear Biometrics, citeseerx.ist.psu.edu/viewdoc/download?doi = 10.1.1.96.6204&rep…

[4] Cavoukian Ann: Privacy and Biometrics, https://www.pcpd.org.hk/english/infocentre/files/cakoukian-paper.doc

[5] Cavoukian, Ann: Biometric and Policing (1999), Comments from a Privacy Perspective.

[6] Daugman J., *How Iris Recognition Works*, IEEE Trans. On Circuits nd Systems for Video Technology, Vol. 14, No 1, pp 21-30, January, 2004.

[7] Gerrit Bleumer, Biometric Authentication and Multilateral Security; In Gunther Muller, Kai Rannenberg (eds.): Multilateral Security in Communications, Addison Wesley, Munchen 1999, 157– 172 (ISBN 3827313600).

[8] http://www.cam.ac.UK.

[9]http://www.eschoolnews,com/showstory.cfm?ArticleID=2146.eSchoolNewsonline.April26,2001.

[10] Marc Gaudreau (1999), "On the distinction between Biometrics, and Digital Signatures" CIC Enterprise Solutions http://www.cic./enterprise/whitepapers.asp.

[11] Mark S. Nixon and John N. Carter (2005), *On gait as a Biometric*: Progress and Prospects.

[12] Murray M. P. et al (1964), *Walking Patterns of Normal Men*, Journal of Bone and Joint Surgery, 46-A(2), pp 335 – 360.

[13] National science and Technology Council (NSTC) subcommittee on Biometrics "Dynamic Signature" 7 February 2006.

[14] Nixon M. S., et al (1999), Automatic Gait Recognition In: A. K. Jain, et al Eds. Biometric Personal Identification in Networked Society, pp 231-250, Kluwer.

[15] NSTC subcommittee on Biometrics "Biometrics overview" 7 February 2006

[16] NSTC subcommittee on Biometrics "Speaker Recognition" 7 February 2006.

[17] Podio F. L. et al (2000), Common Biometric Exchange File Format(CBEFF), NISTIR 6529.

[18] Santos M. , Queiloscopy – *A supplementary Stomatological Means of Identification*. International Microform J. Legal Medicine. 1967; 2.

[19] Uma Maheswari T. N., Lip Prints. A dissertation submitted to The Tamil Nadu Dr. M. G. R. Medical University, Chennai. Degree of Master of Dental Surgery, February, 2005. University of Cambridge, http://www.cam.ac.uk

[20] Winter D., The Biomechanics and Motor Control of Human Gait, 2nd Ed., Waterloo, 1991.

[21] Zdenek Riha and Vaclav Matyas (2000), Biometric Authentication Systems, FIMU Report Series.