BIOMETRIC RECOGNITION: OVERVIEW AND APPLICATIONS

ILOANUSI, O. N [1]
oniloanusi@yahoo.com

OSUAGWU C. C [1, 2]
[1] *Department of Electronic Engineering, Faculty of Engineering, University of Nigeria Nsukka. Enugu State. Nigeria.*
[2] *Computer Communication Centre, University of Nigeria Nsukka. Enugu State. Nigeria.*

ABSTRACT
Earlier forms of person identification or verification like usernames, passwords or personal identification numbers (PINs) are still in use though not sufficiently effective in handling Internet crimes, frauds and security threats. Biometric person identification is preferred because biometric identifiers are unique to each person, permanent and hardly subject to change. These advantages make biometric recognition the preferred mode for most virtual and access control. Biometrics is universal and easily implemented with existing or new technologies. This paper discusses biometric recognition; the different modalities of biometric recognition technology; their strengths, limitations and applications.

KEYWORDS: Biometrics, recognition, identification, verification, applications, limitations, strengths, behavioural, physiological.

1 INTRODUCTION

1.1 The Necessity of Biometric Recognition

It has been a fact of life to authenticate persons before granting them access to certain resources. Human recognition is required for certain reasons like identification and registration of persons, law enforcements, border and national security and criminal investigations. People are checked by a recognized property they have, like an electronic user ID or an RFID (Radio frequency Identity). Persons are also authenticated by what they know like a username, password or PIN. The problem with these existing security measures and automated systems is that some can be stolen, passwords and PIN could easily be forgotten, as there are many passwords to cram with the increasing complexity of electronic access to resources. All the security systems mentioned so far can also be shared without the system knowing for sure who is using it. The best offer for user authentication is biometrics.

Biometrics are physiological (biological) traits or behavioural traits in humans, called identifiers, that uniquely classify each human. A biometric is physiological in the sense that it is part of the bodily make up of the person; it is an intrinsic property of an individual whereas behavioural is an extrinsic property acquired through repetition. It is a tendency. Physiological biometrics includes fingerprint, facial geometry, retinal pattern, iris pattern, palm print, hand geometry, DNA. Behavioural include gait, dynamic signature,

keystroke dynamics, voice print and odour to some extent. Biometric recognition is the automated use of these biological or behavioural identifiers to authenticate or recognize humans. Biometric based verification and authentication systems have several advantages over the other existing systems because the biometric identifiers are unique to each person, intrinsic in the person, universal, permanent and not subject to change. It is not possible to steal the life biological trait of a person. Biological traits cannot be shared. Though off-line biological data can be circumvented, the check is always done life.

Biometrics is particularly important in border control, volume control, Internet crime prevention, data and information security, terrorist threat prevention, all virtual and physical access control. Normally, other security measures are taken to prevent these mentioned threats but they are not sufficient and could fail several times. Biometrics is preferred because of its uniqueness, permanence over time, ease of collection, universality and ability to be implemented with existing or new technology.

1.2 Identification versus Verification

Biometrics recognition systems operate in two modes- verification and identification. Verification is different from identification. A verification system simply checks whether a user is who owns the biometric at the point of access to a resource. It is a 1:1 match. It answers the question s the user who he claims to be? In this mode, a person is authenticated and authorised to use a resource if successful.

Identification systems check a users profile against a database of many users to seek a match or non-match. It is a 1: N match [1]. It answers the question s the user enrolled in the database or not? or ho is this user? In Identification the system verifies the user biometric against each and every enrolled template in the database.

Identification can also be of a positive or negative type. The goal of positive identification is to find the user biometric in the database whereas negative identification tends towards not finding the user in the database..

2. HOW A BIOMETRIC SYSTEM WORKS

A biometric system can be viewed as a simple diagram in figure 1. The enrolment phase comprises a series of steps - input acquisition, digital signal processing, feature extraction and enrolment. The recognition process could be either identification or verification. The steps followed here are input acquisition, digital signal processing, feature extraction, verification or identification.

- The input may be the user face, finger pattern, iris, voice, etc.
- The biometric sensing device is specific to the type of biometric in use. The sensor could be a fingerprint life scan device or a hand geometry reader.
- The biometric sample could be a voice print which is an audio signal; a fingerprint, iris scan, facial scan which are all image signals. Images are digital signals of a spatial type. Digital signal processing is essential to filter out noise and have the signal in the pure form. Usually, several filtration techniques and

algorithms are employed to achieve this and prepare the input signal for feature extraction.

- Feature extraction is the process by which salient information in the biometric input that uniquely characterizes the input is extracted from the input. Feature extraction is a dimensionality reduction [2] of the acquired information. The extracted features are hence encrypted and stored as a biometric template in a database or memory chip. Feature extraction is done with the help of some computational algorithms. The extracted biometric data comprise a template.

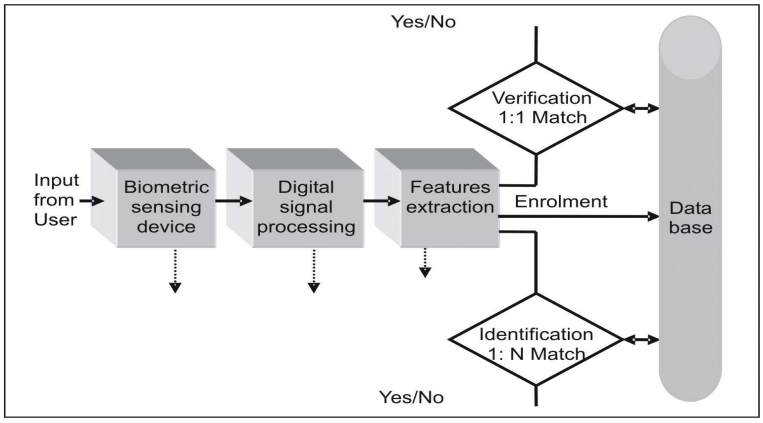

Fig 1: Diagram of Automated Biometric Systems

- Enrolment is the process of registering a user biometric input in a database. It could be an identification database or a memory chip in a card.
- The database is a collection of records of biometric templates of enrolled users.
- The blocks for verification and identification are decision boxes. Verification is a process of checking a user biometric input against a stored biometric and outputting a Yes/No result.
- Identification is the process of verifying a user biometric input against a database of many templates and outputting a present/absent result.
- Finally a decision is taken by a biometric system depending on the set threshold for a biometric decision in the recognition algorithm. A score generated on or above the threshold grants a es and a score below the threshold grants a 'No'.

3. BIOMETRIC TECHNOLOGIES

The automation of the different biometric traits have resulted in various biometric technologies. There are several of them. The fingerprint, iris, retina, palm print, DNA

biometrics are genetically composed within the gestation period of an individual and remain stable throughout one life. Their recognition is based on the principle that no two person biometric are similar, except for the case of monozygotic twins having the same DNA [3].

3.1 Hand Geometry

Hand geometry technology recognizes individuals based on the relations between their certain hand measurements. Though a stable biometric, hand geometry is not as unique or distinctive as fingerprint, iris or retina and hence cannot be used for identification. During enrolment or verification, a hand geometry reader which constitutes a camera, captures the dimensions of the hand [4], and forms an enrolment or matching template. The measurements taken are the thickness, length, width, and distances between fingers and along the curves. It comprises a combination of measurements of the hand length width, thickness, sides and curvatures [5] and can be more than 50 measurements on the whole. The system is a geometrical system and not a pattern recognition system. It simply takes measurements and does not recognize palm or finger prints. In other words, there is no need for image enhancement and features extraction in hand geometry systems.

3.2 Iris

The iris of every human is unique and hence suitable for use as a biometric trait. The iris is genetically composed before birth [6] and remains stable throughout one life, except in the case of an accident. Iris biometric technology recognizes individuals based on the uniqueness of the iris of every person. The iris biometric is acquired through a non-contact process which can range from a distance of 10 to 100cm. In enrolment or recognition, a camera acquires a high resolution image of the iris. Features like striations, rings, furrows are extracted from the iris, and the iris code algorithm converts these features into an iris code template [7] for enrolment or recognition. During enrollment, the iris code is simply stored in the database, whereas in recognition, the iris code is matched against a previously stored iris code in the database to seek a match or non-match.

3.3 Retina

Retina biometric is different from the iris biometric. The retinal biometric is gotten from the complex vein patterns [8] formed at the retina for supplying blood to the eye. The retina of the eye comprises tiny complex capillaries that supply blood to the eye. The network of these capillaries is so complex that no two people have the same retinal pattern, hence unique for every individual. The retina scan is done in real time. It is a contact scan done by positioning the eye in front of the eye scanner for about 15 seconds to make a good scan.

The resulting image is feature extracted, coded and stored as biometric sample or template for verification or identification. This biometric is accurate but not that acceptable as people are not ready to put their eyes through eye scanners each time as the eye is such delicate organ.

3.14 Fingerprint

A fingerprint is an impression of the finger ridge pattern [9] made on a surface or captured with image acquisition device. It is

believed that every human fingerprint is unique. There are no two fingerprints that are exactly the same; not even those of identical twins. Fingerprint patterns remain the same from birth throughout life. When fingerprint ridges are lost through some accidents like burns, abrasions, the same original pattern regrows. Fingerprint is more accurate than face biometric.

Therefore the fingerprint serves as a super biometric that can be used in highly secure systems. Fingerprints can be recognized both in the latent (hidden) form and patent form. Latent fingerprints are dealt with in the area of Forensics. They are called latent because the fingerprints left on surfaces are not visible to the human eye, but can be developed using chemicals in laboratories. In criminal cases, the effective way of catching the suspects is by developing prints deposited in the objects in the scene of crime using suitable chemicals.

Latent fingerprints are more difficult to analyze and automate as patent fingerprints because the analysis of latent fingerprints is qualitative while that of patent fingerprint is quantitative [10]. Latent fingerprint forensic examiners normally do this manually and this takes a lot of useful time.

Patent fingerprints are scanned images of fingerprints for purposes of storing in databases or chips for automated recognition in an AFIS (Automated Fingerprint Identification System) or AFAS (Automated Fingerprint Authentication System) [11]. An AFIS is a database of many fingerprints in which a 1: N matching process is usually done. An AFAS is simply a verification system with a 1:1 match. Live fingerprints are obtained with the help of a live scan device.

The processes involved in obtaining a fingerprint are live scanning, digital signal processing, feature extraction, enrollment or matching.

The fingerprint biometric is relatively a preferred biometric identifier to some others because of its uniqueness, ease of collection, permanence, and cost effectiveness in implementation. Fingerprint biometric systems are robust in design and are open to improvements.

Current trends in fingerprint biometric research include touch less fingerprint devices, 3D imaging of fingerprints, indexing fingerprints, multimodal fingerprint biometric systems.

3.5 DNA (DeoxyriboNucleic Acid)

DNA (DeoxyriboNucleic Acid) is an element that is all over the human body. Every human has a unique composition of DNA except for monozygotic twins. Unlike fingerprints, iris, face that are got automatically using image acquisition devices, DNA acquisition process is not automated. It is acquired biologically and chemically in labs and it takes about four to five hours to obtain a DNA sample. DNA is considered a biometric because of its uniqueness and accuracy. We leave our DNA behind in many things we come in contact with without realizing. Some sources of DNA are paper, glass, dried blood, dried skin, used razor, used tissue, etc.

DNA is effectively employed in Forensics for tracing acquired DNA to their owners. Could be used for crime detection, it is also used for knowing the rightful parents of a child.

DNA is permanent throughout one life and cannot be subject to any change by

accident. DNA tests are difficult to circumvent as the sample is biological and not computer coded.

However, DNA is not suitable for every application because of the privacy issues involved [12]. DNA is so sensitive an information to be used anywhere. The DNA of a person can reveal information about the person family tree, health conditions, future health tendencies and hence quite sensitive to use anywhere.

3.6 Face

Facial biometric technology is the automatic recognition of persons based on some unchanging features unique to every human face. During enrolment or recognition, the facial image is captured by a camera, and unique features like areas around eyes, nose and mouth [13, 14] are extracted to form the enrolment or matching template. The four methods basically employed in recognition of facial images are eigenface, feature analyses, neural network mapping, and automatic face processing [15].

3.7 Palm print

Palm print biometric technology recognizes persons based on their unique palm print patterns [16]. Palm print recognition is similar to fingerprint recognition. However in palm print recognition, more areas can be utilized in composing features for recognition compared to the little area in fingerprints. Recently, some multimodal biometric systems combine fingerprint and palm print or 2D and 3D features [17] of palm prints to improve accuracy of recognition. Palm prints comprise minutiae details, cores and deltas as well.

3.8 The Behavioural Biometrics

The behavioural biometrics for now include gait, dynamic signature, keystroke dynamics, voice, odour. The behavioural biometrics unlike the biological do not have absolute unique identifiers for each person. They can change depending on the mood of the person; hence, the enrolled biometric data of a person may not be the exact as the biometric data of the person under recognition. They are better used for verification.

Gait biometric technology is based on recognition of persons according to their manner of walking [18, 19]. Humans have peculiar way of walking and this serves to distinguish persons. It is still under way to automation.

Dynamic signature technology is a behavioural biometric based on recognizing persons according to their manner of signing signatures. Every individual way of signing signature is distinct, characterized by the stroke, style, pressure of writing and timing between strokes [20].

Keystroke dynamics is based on recognizing persons by their keyboard typing styles or pattern. What is used for recognition is the rhythm of keyboard strokes [21] which vary for each person. It is still under implementation.

Voice biometric technology is the automatic recognition of persons based on their unique vocal characteristics, which is a function of the behavioural and biological aspects of the speech production in persons. The voice of a person is sensed, sampled, processed and recorded as a voice print [22, 23]. The template (voice print) is matched against a user voice online during verification to seek a match.

Odour biometric is used to recognize persons based on their odour which is both biological and physical. Someone odour can

be captured by odour sensors that are effectively sense the unique body chemicals called volatiles [24] in the human body. They are then stored as odour templates/prints.

Other emerging biometrics are vein scan, nail-bed identification, blood pulse, ear shape and facial thermography.

4. WHAT BIOMETRIC: WHERE AND HOW?

The choice of biometric technology used for a certain application depends on the type of access control and the level of security desired. It also depends on the characteristics of the different biometrics. There are some biometric traits more suited for verification than identification and vice versa, or both. Table 1 gives a summary of the strengths and limitations of some twelve biological and behavioural biometric technologies, their recognition mode, security level attainable, and where they can be applied.

Table 1. The strengths, limitations and applications of various biometric technologies.

Biometric Technology	Recognition mode	Strengths	Limitations	Application	Security level
Hand geometry	Verification	→ Cost effective for intended application. → Small template size. → Difficult to circumvent and worthless to forge. → Acceptable because biometric is not sensitive. → Not affected by dirty hands.	→ Not able to do 1:N matching. → Has universal scope of application → Hand can swell	→ Employee monitoring. → Time/Attendance. → Physical logins. → Game resorts	low
Face	Identification Verification	→ handles not only cooperative and non cooperative users. → best for open identification. → more accepted by users. → best in preventing terrorism → works in both recognition modes. → biometric not sensitive	→ Can be abused. → Illumination issues. → Identification can be badly open ended. → Error rates not low. → Not as permanent as iris. Face can wrinkle. → Large rotation angles.	→ Surveillance → Terrorism prevention → Immigrations. → Civil authorities. → Watch list databases.	high
Voice	Verification	→ Not as sensity → Difficult for an impostor to forge all the features of the vocal cord of a person.	→ Not for a wide spectrum of applications. → High error rates. → Voice can be affected by health, emotions. → Not suitable for 1:N identification.	→ E-banking → Online purchasing → Telephone enabled applications → Home security	high

Biometric Technology	Recognition mode	Strengths	Limitations	Application	Security level
Iris	Identification verification	→ Most accurate biometric → Lowest FAR [3] (1 eye; 1 in 1.2M: 2 eyes; 1 in 1.44M) → 0% FRR → Has more features and pattern is stable throughout life time → Best and fastest speed in 1:N identification → High resolution image → Not affected by eye glasses or contact lenses	→ Biometric is sensitive → Applications not as widely spread as fingerprint	→ International passports → Airport → E-banking, ATM → Insurance → Voting	very high
DNA	Identification Verification	→ Image exact when sensed → Low error rates → accurate	→ Same for mono-zygotic twins → Reveals highly sensitive information about user → Not automated → Difficult to integrate into existing technologies	→ Forensics → Crime investigation → Tracing a person to a relative	Very high
Retina	Identification Verification	→ Image exact when sensed → Low error rates → accurate	→ Not as permanent as iris. Eye diseases and health conditions affect pattern → Not acceptable as a regular biometric because or IR rays	→ Physical access control → Immigrations	high
Fingerprint	Identification Verification	→ Deployed in a wide variation of applications, quite universal → Very easy to integrate into most existing technologies (USB, plug and play) → Lower error rate than face → Used in both modes → Permanent biometric → Convenient and cheapest → Dynamic 1:N matching → Very useful in Forensics; best after DNA	→ Biometric can be compromised in online applications. → Not as accurate as iris → Latent fingerprints can be smudged	→ Virtual and physical access control → Property protection → Forensics → Crime investigation → AFIS, AFAS → FBI, CIA → Voting → Handheld devices	high
Biometric Technology	Recognition mode	Strengths	Limitations	Application	Security level

Palm print	Identification	→ Large identification area [4] → Cost effective in identification	→ Smudged prints pose a problem	→ Forensic → Crime investigation	high
Gait	Verification	→ Acceptable to users → Biometric not sensitive → Difficult to forge all dynamic aspects of a person's gait	→ Subject to change → Gait can be faked → Affected by age, health, emotion	→ Surveillance → Physical access control	medium
Dynamic signature	Verification	→ Easy to integrate into applications that involve signing signatures → Difficult to forge all dynamic aspects	→ Can be affected by nervous illnesses → Can be affected by weakness in old age	→ Desktops → Sales, purchases	medium
Keystroke dynamics	Verification	→ Cheap and convenient when integrated into applications involving keyboard input → Convenient adjustment of threshold at individual level → Continuous verification	→ People with typing disorders may be falsely rejected → Moods can affect typing	→ Desktops → Laptops → Hand held devices → Palmtops	medium
Odour	Verification	→ Acceptable to users → Biometric is not sensitive	→ Drugs or medications can affect odour → Weather, environment can affect odour	→ Physical access control	low

5. CONCLUSION

In this paper, aspects of biometric person recognition were discussed. The various physiological and behavioural biometric modalities were explained. The strengths, limitations current and future applications of the various biometric modalities were detailed. This paper would serve as a proper reference for any reader interested in having a global view of biometric recognition.

REFERENCES

[1]. Biometrics - Wikipedia, the free encyclopedia en. wikipedia. org/ wiki/ Biometrics. Last updated on May 22 2009.

[2]. Feature extraction. In: Wikipedia, the free encyclopedia. en.wikipedia.org/wiki/ Feature_extraction. Last modified on 19th May 2009.

[125]. DNA as a Biometric Identifier. Findbiometrics.com: Complete identification verification resource. Accessed on 23rd May 2009 from www. findbiometrics. com/ article/54

[126]. Veldhuis, R., Bazen, A., Booij, W., Hendrikse, A.: A Comparison of Hand-Geometry Recognition Methods Based on Low- and High-Level Features. pp. 326--330. (2001)

[127]. NTSC Subcommittee on Biometrics. Hand geometry. Pp 1 7. http://www. biometrics. gov/Documents/HandGeometry.pdf Last updated 7th August 2006.

[128]. FindBiometrics.com: Complete Identification Verification Source. Understanding Iris Recognition.

[129]. Bowyer, K., Flynn, P., Hollingsworth, K., Baker, S., Ring, S.; oward the next generation of iris biometrics science 4 May 2009, SPIE Newsroom. DOI:

10.1117/2.1200904.159. http://spie.org /x34719.xml?ArticleID=x34719

[130]. Wikipedia, the free encyclopedia, Retinal scan. Last updated 20 May 2009 http://en.wikipedia.org/wiki/Retinal_scan

[131]. Wikipedia, the free encyclopedia, Fingerprint. Last updated 23 May 2009 http://en.wikipedia.org/wiki/Fingerprint

[132]. Jain, A.K.; Jianjiang Feng; Nagar, A.; Nandakumar, K.: n matching latent fingerprints Computer Vision and Pattern Recognition Workshops, 2008. CVPRW apos;08. IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Volume , Issue , 23-28 June 2008 Page(s):1 - 8

[133]. Bhanu, B., Xuejun T.; Computational Algorithms for Fingerprint Recognition 2004 p.9

[134]. Faundez-Zanuy M, rivacy issues on biometric systems In Aerospace and Electronic Systems Magazine, IEEE. Volume 20, Issue 2, Feb. 2005, pp. 13 - 15

[135]. Lee, Y. Yi, T. D face recognition using multiple features for local depth information Video/Image Processing and Multimedia Communications, 2003. 4th EURASIP Conference focused on Volume 1, July 2003 pp 429 - 434 vol.1

[136]. BiometricNEWSPORTAL.COM. ace Biometric http://www.biometricnewsportal. com/face_biometrics.asp

[137]. Chengjun, L., Wechsler, H. ndependent component analysis of Gabor features for face recognition In IEEE Transactions on Neural Networks. Volume 14, Issue 4, July 2003 pp. 919 928.

[138]. Wei, S., Zhang, D. almprint verification: an implementation of biometric technology In Proceedings of the Fourteenth International Conference on Pattern Recognition. Volume 1, Issue , 16-20 Aug 1998 Page(s):219 - 221 vol.1

[139]. Aggithaya, Vivek K.; Zhang, D., Luo, N., multimodal biometric authentication system based on 2D and 3D palmprint features Proceedings of the SPIE, Volume 6944, pp. 69440C-69440C-9 (2008).

[140]. Nixon, M. S., Carter, J. N., n Gait as a Biometric: Progress and Prospects In LNCS Proceedings. Volume 2688, pp 725-733, 2003 www.eurasip.org/Proceedings /Eusipco/Eusipco2004/defevent/papers/cr1922.pdf

[141]. Havasi, L., Szl ik, Z., Szir yi, T.: Detection of Gait Characteristics for Scene Registration in Video Surveillance System. In: IEEE Tr. Image Processing, pp 1--5. IEEE (2006)

[142]. NTSC Subcommittee on Biometrics. Dynamic Signature. http://www.biometrics.gov/Documents/DynamicSig.pdf Last updated 7th August 2006.

[143]. Jain, A.K.: Biometric Authentication based on Keystroke Dynamics. http://biometrics.cse.msu.edu (2001)

[144]. FindBiometrics.com: Complete Identification Verification Source. n Application of Biometric Technology: Voice Recognition http://www.findbiometrics.com /Pages/feature%20articles/voice-recog.html

[145]. International Biometric Group. oice Recognition: How it Works http://www.biometricgroup.com/reports/public/reports/voice-scan_tech.html

[146]. Matyas, J. V., R a, Z.: iometric Authentication Systems FIMU Report Series. FIMU-RS-2000-08 historical.ncstrl.org/tr/pdf /ercimcrcim/2000-FIMU-RS-2000-08.pdf