BIOMETRICS: A SCIENTIFIC WEAPON FOR TACKLING IDENTITY MANAGEMENT CHALLENGES IN NIGERIAN SPORTS DEVELOPMENT.

[1]Ajala, A. O., [2]Falola, K. O., [3]Bolarinwa, O. M.
[1]Department of Management Studies, Nigeria Institute for Sports, Surulere, Lagos, Nigeria
[2]Federal Science and Technical College, Ijebu Imusin, Ogun State, Nigeria
[3]Department of Human Kinetics and Health Education, Faculty of Education, Ekiti State University, Ado Ekiti, Nigeria
Corresponding Author: falolaken@yahoo.com. Tel: +2348029186108

ABSTRACT

Identity management is an important aspect of human life. Today, the world is faced with myriads of identity problems which make people to commit various crimes undetected. Most sports competitions have been marred by fake identities, which have led organizers into honoring wrong teams and athletes, thereby having adverse effects on overall sports development. This paper looks at the proper and effective application of biometrics as a scientific weapon to tackle identity problems in our sports meets. It analyses the potency of the device and how it is capable of putting the problem under control. It concludes that if there is a properly designed database system whereby the biometrics of athletes can be effectively captured, stored, accessed and verified anytime and anywhere, there will be a tremendous success in the battle against identity problems in sports meets in Nigeria.

Keywords: Biometrics, Identity, Cheating, Verification, identification

INTRODUCTION

Identity management is an important aspect of human life. Individuals, families, communities, nations and others have certain attributes that give them their identities which enable a person to differentiate them. Even inanimate objects are associated with signs and traits that distinguish them. The socio-economic and industrial development of a nation needs a sound identification management and formidable national security technologies, most especially at this age of high-level sophisticated crimes and terrorism. The world is indeed ripe for a solid and reliable global identification management. As a country grows in size (population), it becomes increasingly necessary to monitor the identity of every individual so as to be able to ensure a uniform development of all via equal distribution of wealth and opportunities among the populace. To this end, the importance of identity management cannot be overemphasized.

Without doubt, the world is faced with identification problems which make people to commit various crimes undetected. Crimes ranging from armed robbery, kidnapping, violent attacks, genocide, ambush, terrorism and etc have been committed with reckless abandon with little or no solution in sight. Most of the perpetrators of these crimes have gone scot free as a result of poor identity management across the world especially in the third world countries. According to Amil, Arun and Safil (2004) a wide variety of systems require reliable personnel recognition schemes to either confirm or determine the identity of an individual representing their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. Examples of such applications are securing access to sports arenas, buildings, computer systems, laptops, cellular phones and so on. In the absence of robust personal recognition schemes, those systems are vulnerable to the wiles of impostors.

Identity problems have been with us from time immemorial. This prompted some Africans and some other tribes to apply the use of tribal marks for identification in the olden days. During the period in question, many crimes were committed and they went undetected just like we have it today. It is common

mostly in the third world countries of Africa and Asia. It has indeed negatively impacted these countries' electoral processes among other things as most of them cannot boast of credible electoral transition process. In Nigeria particularly, efforts have been made to control identity management problems through the establishment of the National Identity Management Commission (NIMC) by the Act No 23 of 2007 with the mandate to establish, own and operate, maintain and manage the National Identity, Database in Nigeria, register persons covered by the Act, assign new National Identification Number (NIN) and issue (general multi-purpose card GMPC) to those who are citizens of Nigeria as well as to others legally residing within the country.

In sports, most especially in football, cases abound of various forms of identification problems in form of impersonation, age falsification, double identity etc. This problem has persisted for a long time and sports organizers have battled with it since time immemorial without much success reported Ajala (2019). Cheating relating to fake identities abound in sports meets across the globe and this has hindered uniform sports development. In football, most especially in continental and inter-continental tournaments many countries in Africa, Asia and some other parts of the world have consistently fielded ineligible players through fake identities (Ajala, 2019). This trend has led to the emergence and honoring of wrong teams and athletes by sports competition organizers. Most African countries cannot boast of credible election as a result of double identity and multiple voting. Many crimes go undetected due to the use of poor identity management devices. The use of biometrics has enabled the NIMC to capture the data of as many Nigerians as they have covered. A maximum and effective application of this device will give better results and make it difficult for anybody to claim double identity, reported Kumar, A., Kanhangad, V., and Zhang, D., (2010) and, Kirsten (2020). The potency of the biometric device was also proven by Yaba College of Technology who used it to effectively monitor the screening exercise of examination attendance in the institution. It was a huge success as it saved the institution the pains of running after potential examination fraudsters. (Rufai, Adigun & Yekini, 2012).

The issue of age cheating is a serious problem in football all over the world, especially Africa. Many FIFA organized age-limit football tournaments have been marred by various cases of age falsifications, impersonations etc which always remove the shine from such competitions. Many young intending footballers who would have begun promising careers in the game are always denied and have their positions usurped by these age fraudsters. Detecting the presence of over-age players in age-related tournaments has been a difficult challenge for many sports organizations. "Age-doping" is a form of cheating that involves falsification of information about the age of a player to gain advantage in the sport. This clearly contradicts the ethics of sport and fair play. Until now, the age of competitors has generally been proven by official documents such as birth certificates. In some regions of the world however, births are registered at police stations or rural health clinics, or by village elders. Since births do not take place at established hospitals, their registrations are often delayed because of cultural, religious and climatic reasons. This consequently gives room for falsification.

Danny Almonte's age was claimed to be 1989 by his parents until he was found out to have been born in 1987 after he had played severally in the Little League World Series for his Bronx team in 2001 despite being over the cut-off age for the league (A.P. News 2000). American golfer, Tom Shaw claimed throughout his career on PGA Tour to have been born in December 13, 1942 and later produced another certificate that proved that he was born on the same date in 1938 so as to be eligible for the Senior PGA Tour (now the Championship Tour) in the 1989 season. Illegally altering the condition of playing equipment is frequently seen in sports such as baseball and cricket. For example in baseball, a pitcher using a doctored baseball (e.g. putting graphite or Vaseline on the baseball), and a batter using a corked bat are some examples of this. Circumvention of rules governing the conduct and procedures of a sport can also be considered as cheating (Fagbenle, 2009).

At times, the large distance between a place of residence and a registration "office" can mean days of travel and hence delay.

Thus, the official "birth certificate" may not reflect the actual date of birth. In addition to this phenomenon, there is compelling evidence that some players carry documents that are deliberately falsified. In some competitions, officials' suspicions were raised when an entire team had birthdays in the same month of the year or when numerous players on the team had consecutive serial numbers on their birth certificates. It is also noted that some players appear to have two sets of travel documents, and officials are bemused when players are shopping for teddy bears for their children in an "Under- 16" tournament. All this owes to lack of application of biometrics and a centralized reliable database system. There is clearly a need to put a stop to this unhealthy practice and bring honour to the sport and this can be achieved through an effective application of biometrics (which are becoming smarter and more digitalized) as solutions to identification problems in our sports meets (Fashikun, 2011). The safety of participants should also be a thing of concern to organizers of sports meets. The device is expected to provide a way out of security threats at sports venues.

BIOMETRICS IN SPORTS

This refers to the visible behavioural and physiological characteristics that can be measured when verifying a person's identity at any point in time during sports competitions. These characteristics may be physical, physiological and behavioural in nature. They refer to the physical and biological parameters used to identify human beings. Hand geometry, face, iris, retina, body smell, the veins of the hand and fingerprints constitute the physiological, while the gait, how a person walks, how one type on the keyboard, voice and signature are the behavioural characteristics. These can be used to identify a person at any given time, especially during sports meets, recorded Cavoukian and Stolanov (2007). This technology, despite the fact that the innovation has been greatly improved upon over the years needs to cover all the physiological and behavioural traits that can be used for recognition in biometrics. According to Jain, Ross and Pankanti (2006) and Simone (2018), there are seven pillars of biometrics that can be used for identification, and which the traits of a person are usually compared with. They include:

Universality: that is, the trait must be found in every human being. That is, the physical or physiological characteristics must be found in every person.

Distinctiveness: that says that there must be clear and easily noticeable features that can be used to differentiate between the two persons in question.

Permanence: the fact that the traits must be traceable in the person all through his/her lifetime. This means that the traits must be sufficiently invariant (with respect to the matching criterion) over a period of time.

Collectability: that is, the traits must be the ones that can be easily presented quantitatively. That is, it must be measurable.

Performance: that is, how accurately and speedily the system can work to show effectiveness. This shows the achievable recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed.

Acceptability: that is, the fact that the person in question is willing to undergo the test and voluntarily agrees to do it. in essence, it indicates the extent ti which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.

Resistance to circumvention: this talks about how easy or difficult it will be to beat the device, reported Jain, Ross and Pankanti (2004) and Wayman (2006).

Any reliable biometric device must satisfy the required specified recognition accuracy, speed and resource, must be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system. On record, there is no biometric device that can cover all the seven pillars without error. However, some devices will satisfy more of the principles better than the others. For instance, iris and fingerprints will definitely fare better than any other one and will seem more reliable and stronger to use for identification (Jain & Park, 2009).

THE USE OF BIOMETRICS

A biometric system is a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template in the database system. The system/device may work either in verification mode or identification mode, depending on the application context, reported Jain et-al (2004). Even in the educational system in Nigeria, biometric use has been used extensively to tackle the menace of identity problems (Stephen, Chukwudebe and Ezenkwu, 2015)

The Verification mode: this is the one in which the device validates a person's identity by comparing the captured biometric data with his/her own biometric template stored in the database system. Here, the individual claims an identity, usually through a Personal Identity Number (PIN), a user name, a smart card etc, and the system conducts a one-to-one comparison to determine its authenticity. It is usually for positive recognition where the use of same identity by multiple people is prevented. It answers the question of whether the biometric data belong to a certain person or not. A person's identity is authenticated by the biometric device at the verification stage when the newly collected sample biometric data are compared with the one with the corresponding enrolled template. One can store locally e.g. in a database system or a smart card, the template that had been initially registered for future confirmation in a system called one-to-one matching. By this, no athlete can lay claim to another person's identity since a mere punch on the device will let him/her out.

The Identification mode: is used to recognize a person by searching the templates of all the users in a database system for a match. Here, the device is does a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject being having to claim an identity. Identification is a critical component in negative recognition application where the system establishes whether the person who he/she (implicitly/explicitly) denies to be. This is to prevent a single person from using multiple identities Wayman (2001). This is not a positive, but a negative identification because this time, it is applied to prevent a person from claiming multiple identities instead of one. It is also used as for screening people inside a database system to forestall fraud. This is very suitable for identifying a particular sportsman from many athletes available. It answers the question 'Whose biometric data are these?'

Normally, in the modern day identity management, for a person's identity to be conformed, he/she needs to produce his/her PIN or password, cryptographic key, ID card, smartcard etc.(Jain, Bolle and Pankanti, 1999). The security measures above too have their own shortcomings. What could bring problem to these measures include the fact that it is possible to easily forget one's PIN or password, they can be stolen, or they get lost or shared with people. A biometric characteristic is supposed to be part and parcel of a person and so, is another useful material in providing one's identity or 'something you are'. As a result of this, there are some benefits of biometric characteristics which make them better than these security measures mentioned earlier. One, it is not possible to forge them; two, they can neither get lost nor be forgotten; three, they are extremely hard to copy; four, these traits or characteristics are part and parcel of a person, so, to use them, the real owner must be present at the scene and time of usage.

Biometric application has always made it impossible for a person to deny that he has not negotiated a particular spot or made use of a computer set or engaged in a certain business dealings. Truly, the one and only unbeatable of identifying and confirming a person's identity is the use of biometrics as it is being used widely to raise the standard of security and is seen as one of the major panaceas to problems of faked identity among others. Biometric system is expected to be more convenient in usage, faster, more secure, and cheaper to implement and manage than the other traditional methods of identifications and verification of people's identity. Also, biometric devices are capable of stopping blacklisted players who freely find their way into sports competition venues. A blacklisted fan is a fan who is banned from the venue due to disreputable behavior. Without many even realizing it, biometric technology has redesigned the experience of going to a ballgame from start to finish according to Kirsten (2020).

ARCHITECTURE AND DESIGN OF BIOMETRIC RECOGNITION SYSTEM

For a long time now, people have identified one another through the use of voice, face, shape, gait etc, which are the simplest form of identification Simone, (2018). Recently, new and more sophisticated approach brought by the application of biometrics has been a new development for some time now. The steps this device contains and its characteristics vary. There are four main stages of biometrics namely; (i) The Enrollment (ii) The Storage (iii) The Acquisition (iv)The Matching. To use a biometric system, one has to enroll first. A sensor is used to produce a computerized representation of the data collected (e.g. fingerprints) when it comes to using biometric device. Then the important discriminatory characteristics from the computerized representation of the data are collected. They are then used to produce a template, that is, a characteristic data set which is then linked to the person's identity and stored in the system. When next this person presents his/her fingerprints to the sensor, the sample template that has been collected will be compared to the one that had earlier been enrolled with the use of mathematical algorithm. The person's identity is thus confirmed and accepted by the device if they match each other. It is used as simple as that in basic terms, reported Jain, Ross and Pankanti (2006). This was also affirmed by Rufai, Adigun & Yekini (2012 when biometric device was successfully used to screen attendance of students to examination venues to curb illegal entry of students.

A unique feature of the biometric system is the fact that the two templates in comparison need not be necessarily the same for a match to be provided. This is so because two samples of the same biometric from the same individual look totally alike or the same for a match to be provided. This is so because two samples of the same biometric from the same individual look totally alike or the same. This development is called intra user variation brought about by variations in a number of reasons between both sample acquisition times. For example, if there are ambient conditions differences, variations in the person's biometric features etc, these conditions can be experienced. The statistical process with the algorithm that provides a score of the degree of similarity between these two templates presented and compared is called matching. The confirmation of the fact that the two templates are from the same person is improved as the margin score increases. A threshold which determines the margin of error the algorithm can permit regulates the final stage of the process. So, the margin scores must be more than the threshold to suit the purpose of a special application, that is, increasing the threshold makes it to be more fool-proof while decreasing it will make it to be prone to fraud.

COMMONLY USED BIOMETRICS

DNA (Deoxyribonucleic acid): This is a unique code for a person's individuality. But then, identical twins have identical DNA patterns. This clearly is a limitation. It is useful for recognizing a person in forensic applications.

Ear: The ear shape and the structure of the cartilaginous tissues of the pinna are distinctive. Here, the distance of salient points on the pinna are matched from a landmark location on the ear. The features of the ear are not expected to be very distinctive in establishing the identity of an individual.

Face: This is the oldest and most common biometric characteristic used by humans to recognize a person. This recognition is based on two premises namely (a) locating the shape of face attributes like the eyes, nose, eyebrows, lips and chin, considering their spatial relationships and (b) overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. Facial recognition is useful for identifying blacklisted fans who try to gain entry into sports venues Steve.

Facial, hand and hand-face infrared thermo gram: The infrared camera is used to capture the pattern of heat emitted by the human body (which is a unique human characteristic) in an un obstructive way much like a regular photograph.

Fingerprint: This is a pattern of ridges and valley on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are

different and so are the prints on each finger of the same person (Mario, Maltoni, Cappelli, Wayman and Jain, 2002).

Gait: This is the peculiar way one walks, and is a complex spatio-temporal biometric. However, gait is a behavioural biometric and may not remain unchanged, especially over a long period of time due to fluctuations of the body weight, major injuries involving joints or brain due to inebriety.

Hand geometry: This is the measurement of the human hand, taking into consideration its shape, size of palm, length and width of the fingers.

Iris: This is the annular region of the eye bounded by the pupil; and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. This is considered to be one of the most reliable traits for identification.

Keystroke: It has been proven scientifically that each person types on the keyboard in a characteristic way. Although this is behavioural biometric is not expected to be unique to each person but it offers sufficient discriminating information to permit identity verification.

Odour: It is a fact that every object is associated with a characteristic odour of its chemical composition and this could be used to distinguish various objects. A component of the odour emitted by a human (or any animal) body is distinctive to a particular individual. However, this could be limited by powerful deodorant smell nowadays.

Palm print: The palm, just like the fingerprints have pattern of ridges and valleys. The fact that the palm prints are wider than the fingers makes them to be more distinctive than the fingerprints. They require the use of bulkier and subsequently are more expensive than fingerprint sensors.

Retinal scan: This is adjudged to be the most reliable and secure biometric as it is not easy to change or replicate the retinal vasculature which is rich in structure and is a characteristic of each individual and each eye.

Signature: This is the way a person signs his/her name and is considered to be a characteristic of that individual. It is a behavioural biometric. This may change, depending on physical and emotional condition. As a result, it is not very reliable since it can be forged by a smart fraudster.

Voice: This is a combination of physical and behavioural biometrics. The features of an individual's voice are based on the slope and size of the appendages (e.g. vocal tracts, mouth, nasal cavities and lips) that are used in the synthesis of the sound. These physiological features of the human speech are invariant for an individual. However, the behavioural part of the speech is of a person changes over time due to age, medical conditions (e.g. common cold), emotional state etc. it may thus not be reliable.

By and large, the combination of most of these biometric measures will improve the infallibility of the overall measure to avoid penetration by smart fraudsters. If one does not catch you, another one will. Besides, sports organizers or other users have different devices to choose from depending on the suitability of the one chosen device for their programme.

BENEFITS OF BIOMETRIC DATA IN SPORTS

Biometric data both identifies individuals and verifies individuals' identities. Identification through biometrics helps to answer the question 'who is this person?' However, the device is used rationally. It may be facial recognition, voice, gait fingerprints etc for the verification of peoples' claimed identities Kirsten (2020). Benefits of biometrics in sports include the following among others;

Biometric technology increases spectators' convenience. Biometric products maximize the amount of time that fans spend on the queues. The identifiers are intrinsic in every human; thus using biometric identifiers eliminates the need to remember multiple items such as tickets and credit cards just to attend a game.

Biometric technology promotes safety and security. For example, in 2018, Police used DNA from a genealogy database to close a four-decade old investigation Justin (2018)

Use of biometric data creates a customized spectator experience and promotes innovation. Rapid technological improvement encourages fans to expect digital convenient customer service. For example, some sports venues have individual countries' phone applications ('apps') that boast a variety of functions e.g. directing fans to the shortest lines and providing access to instant replays.

In sports, it helps to frustrate the activities of identity fraudsters. For instance, in the 2009 edition of the Federation of International Football Association (FIFA) Under 17 World cup, more than seventy five percent of the players that would have represented Nigeria got disqualified by biometric device for being over-aged.

Comparison of various Biometric Technologies

Biometric Identities	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odour	H	H	H	L	L	M	L
Palm print	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Keynotes: H –High, M-Medium and L- Low *Arun, Anil and Salil (2004*

APPLICATIONS OF BIOMETRIC SYSTEM

Commercial Application: They include electronic data, data security, e-commercial, internet access, ATM, credit card, cellular phone, PDA medical records managements, physical access control, especially during sports meets, computer network login. They make use of knowledge based systems like ID cards, badges etc.

Government applications: They include National ID card, correctional facility, driver's license, social security, welfare disbursement, border control, passport control etc. they make use of ID cards and badges.

Forensic applications: They include corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children etc. They rely on human experts to match biometric features.

The application of biometrics in sports will in no small measure help in fighting the problem of fake identity globally, especially in Africa and Asia where the problem is most prevalent. The problem of age cheating in sports that has become almost insurmountable will be reduced to the barest minimum with the application o biometrics. Cheating thrives only when biometric devices are not properly applied and appropriately monitored. The use of biometrics has been extremely effective and reliable in sports in other parts of the world except in Africa and Asia where the approach to the use of the device coupled with the inconsistency of the application which have made it look unreliable. A proper application and enforcement of the device in sports competitions and other various spheres of life will significantly reduce the problem of age cheating and give room for a level playing ground in sports. Election fraud will become minimal as double voting will be checkmated. Besides, crime rate will considerably reduce in our society. The menace of multiple voting during elections into various sports federation executive bodies will be a thing of the past if biometrics are applied in a proper manner.

CONCLUSION

The application of biometric will in no small measure help in fighting the problem of fake identity in our sports arena globally, especially in Africa and Asia where the problem is most prevalent. The problem of age cheating which has become almost insurmountable will be grossly reduced with the proper application of biometrics as part of the measures against its prevalence. Cheating thrives only when biometric device is not properly applied and appropriately monitored. The use of biometrics has been extremely effective and reliable in other parts of the world except in Africa and Asia where the approach to the use of the device coupled with the inconsistency of the application have made it look unreliable. A proper application and enforcement of the device in sports arena and other various spheres of life will significantly reduce the problem of fake identity which age cheating is an offshoot of, and threats of terrorist attacks will be grossly reduced. This will give room for a level playing ground in sports. Election fraud will become minimal as double voting will be checkmated. Besides, crime rate will considerably reduce in our society. The menace of multiple voting during elections will be a thing of the past if biometrics are applied in a proper manner.

RECOMMENDATIONS

Government should intensify efforts to enforce the use of biometrics for recruitment by our various sports clubs in order to ensure that their youth teams are youths indeed.

There should be a central database system that will be easily accessible at any point in time anywhere and whenever a person tries to claim a particular identity during a sports competition. This should be applicable to all public undertakings including voting during elections.

Government should be prepared to invest on the acquisition of sophisticated gadgets that can match modern day demands to undertake the conduct of biometrics and data registration. In the developed countries, ordinary portable devices are used to easily bring out anybody's identity as long as the person's data have been taken and imputed into a central database system.

References

Ajala, A.O. 2019. Administrative measures in curbing age-cheating in competitions among football players in Nigeria. An unpublished doctoral thesis submitted to the University of Ibadan.

Cavoukian, A. and Stoianov, A. 2007. *Biometric encryption: a positive-sum technology that achieves strong authentication, security and privacy.* Information and Privacy Commissioner/Ontario, Toronto, p48. Retrieved from: http//www.ipc.on.ca/image/Resources/bio-encryption. On: 6th February, 2008.

Dvorak, J. 2009. Detecting overage players using mri: science patnering with sport to ensure fairplay.

Jain, A.K., Bolle, R. & Pankanti, S. 1999. Biometrics: Personal identification in networked society. Kluwer. Kluwer Academic Publishers.

Jain, A. K., Ross, A., and Prabhakar, S. 2004. An introduction to biometric recognition. .I. E.E.E. *Transactions on circuits and systems for video technology.* 14. 1: 4-20

Jain, A.K., Arun, R. & Salil, P. 2004. Special issue on image-and video-based biometrics. *An Introduction to Biometrics Recognition.* 14. 1.

Jain, A. K., Ross, A and Pakanti, S. 2006.Introduction to biometrics- a tool for information security. I.E.E.E. *Transactions on information forensics and security.* 1. 2: 125-143

Jain, A/K, and Feng, J. 2009. Latent palm print matching. IEEE Trans Pattern Anal Nach Lintel. 31. 6: 1032-1047

Jain, A.K. and Park U. 2009. Facial masks: soft biometrics for face recognition. Proc. Int. Conf. Image Procets. Cairo, Egypt.

Kirsten, F. 2020. The prison of convenience: the need for national regulation for biometric technology in sports venues. *Fordham International Property Media and Entertainment Law Journal.* 30: 3. 5

Kumar, A., Kanhangad, V., & Zhang, D., 2010. A new framework for adaptive multimodal biometrics management: to appear in IEEE Trans Inf Security Forensics. Available online

Maio, D., Maltoni, D. Cappelli, R., .Wayman, J.L. & Jain, A.K. 2002. Fingerprint verification competition. Quebec City. *Proc. International Conference on Pattern Recognition (ICPR*) PP 744-747.

Rufai, M.M., Adigun, J.O., and Yekini, N.A. 2012. A biometric model for examination screening attendance monitoring in Yaba College of Technology. *World of Computer Science and Technology Journal (WCSIT) 2: 4. 120-124*

Simeone, C. 2018. Biometrics and personal identity: an alternative and philosophical approach to the mainstream debate. An unpublished work submitted to the Faculty of Behavioural Management and Social Sciences for the award of master's degree in Philosophy of Science, Technology and Society, University of Twente, Netherlands.

Stephen, B.U., Chukwudebe, G.A. and Ezechukwu, C.P. 2015. Integrated identity and access management system for tertiary institutions in developing countries *Nigerian Journal of Technology.* 34: 4. 830-837.

Wayman, J.L. 2001.Fundamentals of biometric authentication technologies. In J. L. Wayman ed. *National Biometric Test Center Collected Works* 1997-2000. Version 1:2. San Jose.