Contemporary Tools In Forensic Investigations: The Prospects And Challenges

S Adebisi

Citation

S Adebisi. *Contemporary Tools In Forensic Investigations: The Prospects And Challenges*. The Internet Journal of Forensic Science. 2008 Volume 4 Number 1.

Abstract

Forensic practice had of recent time gone beyond just identification and tracking down criminals, but now to prevent the incidence, considering the advancing technology being presently employed. It is nonetheless obvious that such frantic efforts are no more fool-proof, or foul-proof, with attending record of fraud, less reliance and safe and hence, unsecured. This paper reviews some of the existing ventures with the opinion to admit failure yet, and considering search for a possible, better biological marker that could function with less or no technological aids, or in the lack of such bio-marker, to keep advancing on a possible perfection of the yet available techniques.

INTRODUCTION

Forensic scientists examine evidence from crime scenes in an effort to solve crimes. They study those aspects of human parts useful in identification of an individual in order to testify before the law. Such useful aids of identification include among others: skeleton, fingerprints, iris, facial scans, hair, blood and DNA match. Forensic means legal, a word that comes from Latin, meaning ‘to the forum.’ The forum was the basis of Roman law and was a place of public discussion and debate pertinent to the law (1, 2).

Indeed, forensic science had come a long way. It had evolved through the ages when fingerprints were found in early paintings and in rock carvings of prehistoric humans. In Lancaster, England in 1784, John Toms was convicted of murder on the basis of the torn edge of wad of newspaper in a pistol matching a remaining piece in his pocket. This was one of the first documented uses of physical matching. In early the 1830’s, Adolphe Quetelet, a Belgian statistician, provided the foundation for Bertillon's work by stating his belief that no two human bodies were exactly alike, and soon after, in 1880, Henry Faulds published a paper suggesting that fingerprints at the scene of a crime could identify the offender. In one of the first recorded uses of forensics to solve a crime, Faulds used fingerprints to eliminate an innocent suspect and indicate a perpetrator in a Tokyo burglary. In 1915, the International Association for Criminal Identification, (to become The International Association of Identification (IAI), was organized in Oakland, California; and in 1984, Alec Jeffreys first used DNA to solve a crime, identified Colin Pitchfork as the murderer of two young girls in the English Midlands. Significantly, in the course of the investigation, DNA was first used to exonerate an innocent suspect (3).

FORENSIC ANTHROPOLOGY

Forensic anthropology is a sub-discipline within the subfield of physical anthropology. Forensic anthropology is an applied area. It borrows methods and techniques developed from skeletal biology and osteology and apply them to cases of forensic importance. Methods and techniques such as anthropometry to assess age, sex, stature, ancestry, and analyze trauma and disease are generally developed to help anthropologists understand different populations living all over the world at different times throughout history. Anthropometry deals with the quantitative assessment of human/animal physiques (4).

Forensic anthropologists frequently work in conjunction with forensic pathologists, odontologists, and homicide investigators to identify a decedent, discover evidence of trauma, and determine the postmortem interval. Though they typically lack the legal authority to declare the official cause of death, their opinions may be taken into consideration by the medical examiner. They may also testify in court as expert witness, with evidences such as forensic facial reconstruction. (5)

A forensic anthropologist may be called in when human

remains are found during archaeological excavation, or when badly decomposed, burned, or skeletonized remains are found by law enforcement or members of the public. The anthropologist can assess metric and non-metric characteristics of the bones to determine the minimum number of individuals, sex, stature, age at death, time since death, ancestry and race, health, and unique identifying characteristics such as healed breaks or surgical scars. Sometimes the forensic anthropologist must determine whether the remains found are actually human. Occasionally, positive identification can be established from such remains, but often only an exclusionary identity can be drawn. In skeletal trauma analysis, some forensic anthropologists can accurately determine whether sharp force, blunt force, or ballistic injury occurred before death (antemortem), near the time of death (perimortem), or after death (postmortem). By examining the marks left on bone, particularly skilled forensic anthropologists may be able to determine general class characteristics of the weapon used. A forensic anthropologist's analysis of skeletal trauma can assist the Medical Examiner in determining cause and manner of death (natural, accidental, homicide, suicide). Even cremated remains can provide a surprising amount of information about the deceased individual (6).

The question of racial affiliation is difficult to answer because, although racial classification has some biological components, it is based primarily on social affiliation. Nevertheless, some anatomical details, especially in the face, often suggest the individual's race. In particular, white individuals have narrower faces with high noses and prominent chins. Black individuals have wider nasal openings and sub-nasal grooves. American Indians and Asians have forward-projecting cheekbones and specialized dental features. One vital tool in the assessment of metric skeletal characteristics is the Fordisc program, which allows the forensic anthropologist to match specific characteristics to a racial or ethnic profile or compared with such figures in the following tables using Discriminant Function Analysis (DFA) to determine the race (6, 7)

The comparative craniometric values (mm) of the skull in some world races (8, 9)

tbl1

Table 2. The mean comparative diameter (mm) of femoral head in some races (10)

The usefulness of bones in identification was confirmed from the old saying that ‘dead men do tell tales’ borne out in a remarkable French murder case in which a skeleton gave up sufficient of its secrets to identify the victim and trap a pair of murderers. In 1889 police were called to a riverside location near Lyons where the badly decomposed body of a man had been discovered. Close by was a decayed wooden trunk bearing evidence that it had been sent to Lyons from Paris by railway. Monsieur Goron, Chief of the Surete, thought the corpse might be that of a Paris bailiff, a man called Gouffe, who had been reported missing. One of Gouffe's relatives was asked to view the remains, but as he was unable to make any identification the corpse was buried. Convinced that a crime had been committed, Boron obtained an exhumation order and three months after it was discovered the corpse was disinterred. The post-mortem examination was carried out by Alexandre Lacassagne, Professor of Forensic Medicine at Lyons University who confirmed it was Gouffe. (11)

FINGERPRINTS

The science of fingerprint identification is one of the most commonly used forensic tools available to law enforcement agencies around the world where utilization of this science allows investigators to recover latent prints from crime scenes and items of evidence. Because the surfaces that fingerprints can be left on will vary, so must the techniques you use to recover them. There are also various techniques to deal with the different substances that a print can be left in such as blood, sweat, or anything that is soluble enough to make its way between the ridges on your fingertips. Recovering these prints is only the first half of making identification. To positively identify the owner of the prints one must compare the prints in question to those of a known individual by methodically analyzing them through the process of analysis, comparison, evaluation and verification. This is done by analyzing the pattern type and individual characteristics that are formed by the ridges on friction ridge skin (12).

The Automated Fingerprint Identification System (AFIS) is crucial in identifying fingerprints left at crime scenes, known as latent (hidden) prints, in the attempt to solve crimes. The fingerprint expert uses a variety of powders, chemicals, lighting, and photographic techniques to make a latent print visible on physical evidence, and then records it permanently. Specially trained Latent Print Examiners search the latent fingerprint against the AFIS Database in an attempt to identify the person whose print was left at the crime scene. In order to prepare a latent fingerprint for an

AFIS inquiry, the examiner digitally scans a latent 'lift' or a photograph of a latent print from physical evidence into a personal computer and enhances the image by adjusting the properties of the image, such as contrast, color, and density. The Latent Print Examiner traces out the ridges including the identifying characteristics using specific graphic techniques and then makes a printout of the tracing to initiate a search against the AFIS Database. The computer produces a list of possible matches, which are compared by the Latent Print Examiner for positive identification. In the event of a possible match or 'hit,' the Latent Print Examiner verifies the 'hit' by checking the latent print against the corresponding inked or Live Scan-captured Ten-Print Card and notifies the detective in charge of the case. If a match is not found, the latent print is then registered to the Unsolved Latent Database. This database is searched every time a new Ten-Print Fingerprint Card is added. (13)

The Integrated Rapid Imaging System (IRIS) for the digital capture of fingerprints in police laboratories (IRIS) consists of a scientific grade digital camera integrated with forensic light sources and infra-red and fluorescent filter. It is capable of capturing fingerprints developed using all current fingerprint development techniques. The digital capture system eliminates time-consuming conventional photography and subsequent processing and has significantly reduced turnaround times and backlogs in laboratories where it has been installed. In the United States for instance, Images are stored with a full audit trail and can be quickly transferred to Ident1, the national fingerprint database. Images can also be imported from scene of crime cameras and rescaled for input to Ident1. There are currently twenty five IRIS workstations in use in the UK, some capturing in excess of 100 fingerprints every day (14)

However, contact issues can affect the sample provided to the fingerprint sensor when an elderly user presents a fingerprint to the fingerprint device. Due to effect of ageing, the skin becomes drier, the skin sags from loss of collagen, and the skin becomes thinner and loses fat as a direct result of elastin fibers. All of these decrease the firmness of the skin, which affects the ability of the sensor to capture a high quality image. The skin of elderly individuals is likely to have incurred some sort of damage to the skin over life of the individual. Medical conditions like arthritis affect the ability of the user to interact with the fingerprint sensor. All of these factors inevitably affect the quality of the sample provided to the fingerprint sensor (15, 16, 17, 18)

DNA PROFILING

To identify individuals, forensic scientists scan 13 DNA regions, or loci, that vary from person to person and use the data to create a DNA profile of that individual (sometimes called a DNA fingerprint). There is an extremely small chance that another person has the same DNA profile for a particular set of 13 regions. Deoxyribonucleic Acid - the fingerprint of life also known as DNA was first mapped out in the early 1950's by British biophysicist, Francis HarryCompton Crick and American biochemist James Dewey Watson. They determined the three-dimensional structure of DNA, the substance that passes on the genetic characteristics from one generation to the next. DNA is found in the chromosomes in the nucleus of a cell. Every family line has its own unique pattern of restriction-enzyme DNA fragments. This variation in patterns of DNA fragments found in human genetic lineages is called 'restriction-fragment length polymorphism' (RFLP). Because each person, except for identical twins (which have the exact same DNA), is formed from two family lines, the pattern of sizes of the fragments from an individual is unique and can serve as a DNA fingerprint of that person (19).

These 'fingerprints' have become very important in identifying criminals in a number of violent crimes where the victims aren't able to. Knowing your DNA fingerprint not only can tell you about the origins of your ancestors but also explain the physical appearance that you or your relatives may possess (hair, eye color, morphology, physiognomy and the like). Unlike other autosomal tests, the World Match DNA Fingerprint Test computes the likelihood of its matches on the basis of contemporary populations, not ancient world migrations or evolutionary theory. And it is not confined to just your two 'outside' male-male or female-female lines. Thus, in many people's opinion, its results are more practical, accurate and realistic.(19, 20)

A fascinating discovery was when researchers for the first time identified human DNA in household dust — a breakthrough which they claim could be used in future to trap murderers and thieves by proving their presence at a crime scene at a certain time; according to the researchers, further study could find ways of recreating someone's profile or even working out how recently they'd visited a crime scene from the decay of their DNA. Brown and his colleagues at Virginia Commonwealth University in Richmond collected dust samples from various rooms around their campus, from highly trafficked classrooms to quieter offices. Most of the DNA they recovered came from

bacteria or fungi, but there was human DNA in all except one of their 36 samples, though each sample contained just trillionths of a gram of DNA, it was more than enough for amplification and profiling via the DNA kits used in forensic labs, according to the Virginia team (19, 27)

FACIAL SCAN

A computer modeling system for facial reconstruction has been developed that employs a touch-based application to create anatomically accurate facial models focusing on skeletal detail. A research had been designed that discussed the advantages and disadvantages of the system and illustrates its accuracy and reliability with a blind study using computed tomography (CT) data of living individuals. Three-dimensional models of the skulls of two white North American adults (one male, one female) were imported into the computer system. Facial reconstructions were produced by two practitioners following the Manchester method. Two posters were produced, each including a face pool of five surface model images and the facial reconstruction. The face pool related to the sex, age, and ethnic group of the target individual and included the surface model image of the target individual. Fifty-two volunteers were asked to choose the face from the face pool that most resembled each reconstruction. Both reconstructions received majority percentage hit rates that were at least 50% greater than any other face in the pool. The combined percentage hit rate was 50% above chance (70%). A quantitative comparison of the facial morphology between the facial reconstructions and the CT scan models of the subjects was carried out using Rapidform™ 2004 PP2-RF4. The majority of the surfaces of the facial reconstructions showed less than 2.5 mm error and 90% of the male face and 75% of the female face showed less than 5 mm error. Many of the differences between the facial reconstructions and the facial scans were probably the result of positional effects caused during the CT scanning procedure, especially on the female subject who had a fatter face than the male subject. The areas of most facial reconstruction error were at the ears and nasal tip (21, 22)

More so, there is presently an invention that relates to creation of a forensic skull and soft tissue database and on-line facial reconstruction. This invention improves the forensic accuracy of facial reconstruction of unidentified victims and age progression of missing children, and expands the database of soft tissue thickness' in multiple ethnic groups and both sexes, as well as other factors such as weight and bone density, through the use of computer and medical imaging technology.(23)

IRIS SCAN

Iris scanning can seem very futuristic, but at the heart of the system is a simple CCD digital camera. It uses both visible and near-infrared light to take a clear, high-contrast picture of a person's iris. With near-infrared light, a person's pupil is very black, making it easy for the computer to isolate the pupil and iris (24).

When you look into an iris scanner, either the camera focuses automatically or you use a mirror or audible feedback from the system to make sure that you are positioned correctly. Usually, the eye is 3 to 10 inches from the camera. When the camera takes a picture, the computer locates: the center of the pupil, the edge of the pupil, the edge of the iris, the eyelids and eyelashes. It then analyzes the patterns in the iris and translates them into a code.(25)

Iris scanners are becoming more common in high-security applications because people's eyes are so unique (the chance of mistaking one iris code for another is 1 in 10 to the 78th power. They also allow more than 200 points of reference for comparison, as opposed to 60 or 70 points in fingerprints. The iris is a visible but protected structure, and it does not usually change over time, making it ideal for biometric identification. Most of the time, people's eyes also remain unchanged after eye surgery, and blind people can use iris scanners as long as their eyes have irises. Eyeglasses and contact lenses typically do not interfere or cause inaccurate readings. Imagine being able to go to an ATM to withdraw money without the need for a card or a password. You simply look into an ATM camera, which detects the pattern of the specks on your iris and releases funds from your account. The convenience of this technology is not limited to your banking transactions. Proponents of the technology predict that iris recognition systems will soon become popular for use at work, home, and for retail and online purchases.

This technology not only offers convenience, but also promises greater safety and security. Top airport security officials have recently recognized iris identifiers as an important tool for increasing airport security and for improving upon current immigration practices. In the United States for instance, more than 2,100 departments in 27 states are taking digital pictures of eyes and storing the information in databases that can be searched later to identify a missing person or someone who uses a fake name, says Sean Mullin, president of BI{+2} Technologies, which sells the devices. A growing number of sheriff's departments are using iris scans to identify sex offenders, runaways, abducted children

and wandering Alzheimer's patients. He says the level of detail and central database can make matches within seconds, compared with weeks for fingerprints and months for DNA. Iris recognition technology has been used by airports to expedite security checks of low-risk travelers and by the government to track possible terrorists. When a patent expired last year, other companies rushed in to expand its uses. The cameras use harmless infrared light to record the iris' minute ridges and valleys. They can detect 235 unique details and differentiate between right and left eyes and those of identical twins, whereas a fingerprint has about 70 details. Irises aren't affected by age, eye surgery or disease (26).

BLOOD TYPING

Blood Typing is one method forensic scientists use as a way to gather evidence from a crime scene. Although blood typing can not specifically identify one particular individual, it can be used as circumstantial evidence and in conjunction with the total body of evidence. When forensic scientists use blood typing, they are looking for the proteins that may or may not be present on the surface of red blood cells (AB proteins and Rh proteins). There are more than 300 known blood group proteins. An individual can have the following blood types: A (AA or AO), B (BB or BO), AB (AB) or O (OO); Rh+, Rh-. Most blood typing tests require forensic investigators to draw blood from the suspect or suspects and from known individuals (always need a comparison). Forensic investigators look for the presence (or absence) of agglutination (clumping) during antibody-antigen reactions. (27)

HAIR

All mammals (humans, animals, etc.) have hair. Hair functions to insulate the body, act as a sensory device and protect against harmful UV rays. Humans have lost much of their body hair over the course of evolution (possible as a protection against disease causing organisms). Although hair is dead protein, we can gather quite a bit of evidence from hair (trace evidence). Animal hair and human hair (head hair, body hair, pubic hair) are considered both class and individual evidence and, therefore, useful in forensic investigations. Because hair is extremely durable, resistant to decomposition and grows from the skin, we can test for various substances (poisons and toxins) that might be present in the body. Hair grows approximately 1.3-1.5 mm/month and, therefore, can be used as a virtual timeline of events–when did poisoning begin for example or how long has a particular individual been using drug. Neutron Activation Analysis (NAA) is a scientific technique that can be used to give us the probability of two individuals having the same concetration of elements in their hair. In order for us to successfully use hair in forensic investigations, we need to be familiar with the proper use of the compound microscope, structure of both animal and human hair, and racial differences in hair structure. (27)

BIOMETRICS IN FORENSICS

Advancing technological innovations are using human biological information to protect data and data access. Devices built to authenticate or identify an individual based upon biological markers are part of a field of science known as biometrics. A person’s fingerprint whorls and swirls, their hand and face geometry, their iris and retinal patterns, their voice pattern, and even the composition of their sweat are all examples of biometrics. In our daily lives, the act of recognizing another individual requires us to interpret biometric information. Biometrics of the past and present – even those as commonplace as the hand-written signature – are already being enhanced or outright replaced by advancing biometric techniques. Yet many of the elements in biometric research are relatively unknown to the Information Science community. How appropriately these biometric advancements are applied to securing data, their practicality in everyday application, their effectiveness and accuracy, and how heavily we rely upon them to protect data are timely issues. However, in spite of the apparent enormous applications of this novel innovations, cautions must be taken, as there is a great need for more study and research before we allow these newer, more personal, and potentially invasive biometric technologies to enter our lives, because these technologies carry the possibility of becoming so heavily ingrained and accepted in our daily routines that we may find ourselves unable to distance ourselves from them (28, 29, 30, 31, 32, 33)

Biometric technologies have been under development for years. Finger, face, and iris scanners are already in place in both high and low security environments. Over the next decade, many companies are preparing to deploy biometric scanners in everything from cars and pocketbooks to corporate offices and ATMs. The proliferation of a technology that is currently unregulated, non-standardized, and uses questionably secured databases to hold unique, non-secret, and irreplaceable personal identifiers - whether fingerprint, iris, facial scan, or some other - is risky; this especially should be noted by decision makers and influencers who manage data access and those who may

consider implementing or authorizing the use of biometrics in their data environment. The biometric technologies available today are often used for the securing of data and information access – either physical, electronic, or both. Within each type of biometric – facial, finger, palm or ear geometry scanning; iris or retinal imagery scanning; sweat composition measurements; blood DNA matching; etc. – and each biometric type varies in its ability to provide accurate results. (34, 35, 36, 37, 38)

The optical sensors used in some biometric devices, including many fingerprint and palm scanners, often accept forged biometrics because they look only at the physical details, such as fingerprint ridges. This is because optical sensors view the input as a static set of information. These recognition inaccuracies are known in biometrics as 'false positives' and 'false negatives.' Regardless, all biometric technologies tend to focus on one of three applications – authentication, authorization, or identification of an individual. The appropriate usage of an application in a given circumstance is a subject of much debate in the biometric field because biometrics do not perform as well in identification as they do in authentication. Furthermore, biometric applications collect and store unique personal data without proof that the biometric data storage methods are secure against proven attacks and frauds. For instance, iris scanners and facial recognition scanners could be frauded: in a test, researchers took photographs of eyes enrolled in the system and used an inkjet printer to produce photographic quality printouts of them. Once the scanner's method of detecting liveness was determined – eye depth in this case – the researchers found a novel approach to circumvent the test. Unable to get the scanner to accept an image of an eye as real, they cut out and removed the pupil from the printout, then put their own eyes behind the image and thereby fooled the iris scanner. Also, facial recognition scanners fell short of precision to researchers with hand held photographs and replayed AVI video clips that showed a few seconds of a head turning. (39, 40)

CONCLUSION

An important question that now arises is whether or not combining identification and authentication is an improvement in security. A risky benefit of biometric technology is that it is possible to authenticate a biometric against a database without ever identifying the person. Think of a fingerprint as a password that is assumed so unique that it provides access based solely on the approval of that biometric 'password' with no 'username' required. The tradeoff is that the username and password (or identifier and authenticator) are permanently tied together, which means that linking the identifier to the authenticator could be done without the knowledge of the person who supplied it. (41, 42) Hence, it would be right to admit that man and his technology is yet in search of a fool-proof bio-marker and safety device for security and fighting crimes.

References

1. Forensic Anthropology: The thin blue line information section. Information Section: NSW Police Information
2. Terrie Winson. The Forensic Anthropologist Forensic sciences Forensic Anthropology 2008
3. www.history of forensic science. forensic science timeline. Retrieved August 15, 2008
4. Forensic anthropology - Wikipedia, the free encyclopedia
5. American Board of Forensic Anthropology. American Board of Forensic Anthropology, Inc.. Retrieved on August 18, 2008
6. Forensic Anthropology CenterThe University of Tennessee 2008
7. Howells WW Who's Who in skulls: ethnic identification of crania from measurements. Peabody Museum Papers 1995, 82:1-108.
8. Shukla, A.P, Singh, SP, Shamer, S. Morphological and Metrical Analysis of Indian Crania 1973; 12(11) 492-498.
9. Adebisi, S.S. The medical impacts of anthropometric records.
Annals of African Medicine, 2008; 7(1): 42-47
10. Singh, S.P, Ekandem, G.J, Ani, O.E.O. Identification of sex from head of the femur-demarking points for Calabar, Cross River State. West African Journal of Anatomy 1986; 1(1): 16-27
11. Kewal Krishan: Anthropometry in Forensic Medicine and Forensic Science-'Forensic Anthropometry'. The Internet Journal of Forensic Science. 2007. Volume 2 Number 1.
12. Matsumoto, T. et al., "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," Proc. SPIE, vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, 24-25 Jan 2002;
http://dependability.cs.virginia.edu/bibliography/s5p4.pdf.
13. King County Regional Automated Fingerprint Identification System
The Future of AFIS Including AFIS Initiatives 2007-2012 – May 15, 2006
14. Fingerprint and footwear marks. Using IRIS technology. Home Office Scientific Development Branch
15. Fingerprint Identification Systems – Capacitive Sensors," online memo, Bergdata Biometrics GmbH, http://www.bergdata.com/en/technology/capacitive.php.
16. Mnookin, J.L. "The Achilles' Heel of Fingerprints," The Washington Post, A27, 29 May 2004;
http://www.washingtonpost.com/ac2/wp-dyn/A64711.
17. Jain, A.K. and Uludag, U. "Hiding Fingerprint Minutiae in Images,"
Automatic Identification Advanced Technologies (AutoID 2002);
http://biometrics.cse.msu.edu/autoid02-n35-jain-uludag.pdf.
38
18. Proceedings of 6th International Conference on Recent Advancements on Soft Computing (RASC 2006). K. Sirlantzis (Ed..) pp. 449-456
19. http://dnaconsultants.com/Detailed/332.html
20. www.ondix.com
21. A blind accuracy assessment of computer-modeled

forensic facial reconstruction using computed tomography data from live subjects Forensic Science, Medicine, and Pathology. 179 – 187; 2007.
22. De Greef S, Claes P, Mollemans W, Loubele M, Vandermeulen D, Suetens P, Willems G (2005) Semi-automated ultrasound facial soft tissue depth registration: method and validation. J Forensic Sci.; 50(6):1282-8.
23. Haaga, John R. Miller, David A. Molter, Joseph P. Duerk, Jeffrey L.
Lewin, Jonathan S. (2008). Forensic skull and soft tissue database and on-line facial reconstruction of victims and age progession portrait rendering of missing children through utilization of advance diagnostic radiologic modalities
24. Angela Jervis E:\Forensic Evidence_com Identification Evidence-Personal Identification by the Iris of the Eye.htm-Angela
http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml
25. Graczyk, M. "Houston airport using fingerprints, eye scan in security test," USA Today, Aug. 2004;
http://www.usatoday.com/travel/news/2004-08-04-houston-trusted_x.htm?POE=TRVISVA
26. Wendy Koch. Iris scans could be 'as common as fingerprinting' USA TODAY
December 05, 2007
27. Vacca, J. "Biometric Security Solutions," Informit, 25 October 2002;
http://www.informit.com/isapi/product_id~%7BC3A2803B-7E73-4341-AB9F-BC91D275E970%7D/content/index.asp.
28. Wilson, Tracy V. "How Biometrics Works." 11 November 2005. HowStuffWorks.com.
http://science.howstuffworks.com/biometrics.htm 15 September 2008.
29. Vacca, J. "Biometric Security Solutions," Informit, 25 October 2002;
http://www.informit.com/isapi/product_id~%7BC3A2803B-7E73-4341-AB9F-BC91D275E970%7D/content/index.asp.
30. Schneier, B. Secrets and Lies, Digital Security in a Networked World, New York: Wiley Computer Publishing, 2000.
31. Jewell, M. "Database culture ripe for ID theft," Oakland Tribune, 10 Aug 2004;
http://www.oaklandtribune.com/Stories/0,1413,82~10834~2325047,00.html.
32. Clothier, "Biometrics to keep handbags safe," CNN, 28 July 2004;
http://www.cnn.com/2004/TECH/07/26/biometrics.handbag/index.html.
33. Schneier, Beyond Fear: Thinking Sensibly about Security in an Uncertain World, New York: Copernicus Books, 2003, pp.181-206.
34. Soutar, C. "Biometric System Security," tech. report, bioscrypt, 2002;
http://www.bioscrypt.com/assets/security_soutar.pdf.
35. Adler, A. "Images can be Regenerated From Quantized Biometric Match Score Data,"
http://www.site.uottawa.ca/~adler/publications/2004/adler-2004-ccece-quantized-match-score.pdf.
36. Ratha, N.K. "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," IBM Systems Journal, v 40, n 3, 2001; p 614-634.
37. Jain, A.K. Dass, S.C. and Nandakumar, K. "Can soft biometric traits assist user recognition?" Proc. SPIE Defense and Security Symposium, Orlando, April 2004,
http://biometrics.cse.msu.edu/JainDassNandakumar_SPIE04.pdf.
38. Asburn, J. "The Distinction Between Authentication and Identification," Avanti, 2000;
http://homepage.ntlworld.com/avanti/authenticate.html.
39. Uludag, U. and Jain, A.K. "Multimedia Content Protection via Biometrics-Based Encryption," Proc. 2003International Conference on Multimedia and Expo (ICME 2003);
http://biometrics.cse.msu.edu/UludagJain-ICME2003.pdf
40. Jain, A.K. et al., "Biometrics: A Grand Challenge," Proc. International Conference on Pattern Recognition, Cambridge, UK, 2004;
http://biometrics.cse.msu.edu/biometricsgrandchallenge.pdf.
41. Stapleton, J. "American National Standard X9.84-2001 Biometric Information Management and Security." Proc. Biometric Consortium Conference, Feb 13-15, 2002;
http://www.itl.nist.gov/div895/isis/bc2001/FINAL_BCFEB02/FINAL_4_Final%20Jeff%20Stapleton%20Brief.pdf.
42. Thalheim, L. Krissler, J. and Ziegler, P. "Body Check: Biometric Access Protection Devices and their Programs Put to the Test," c't. Nov. 2002: 114;
http://www.heise.de/ct/english/02/11/114.

Author Information

Samuel S. Adebisi, PhD
Human Anatomy Department, Faculty Of Medicine, Ahmadu Bello University, Zaria - Nigeria