₹ 200 ISSN - 2249-555X

Volume : 1 Issue : 6 March 2012

Journal for All Subjects

www.ijar.in

Listed in International ISSN Directory, Paris.

ISSN - 2249-555X

Indian Journal of Applied Research

Journal for All Subjects

Editor,
Indian Journal Of Applied Research
8-A, Banans, Opp. SLU Girls College, New Congres Bhavan, Paldi,
Ahmedabad-380006**,** Gujarat, INDIA
Contact.: +91-9824097643 E-mail : editor@ijar.in

INDEX

Volume : 1 | Issue : 6 | March 2012 ISSN - 2249-555X

Research Paper Law

Application of Biometrics in the Investigation of Crime

* Dr. R. Thilagaraj ** G. Deepak Raj Rao

* Professor & Head, Department of Criminology, University of Madras,Chennai

** Research Scholar, Department of Criminology, University of Madras, Chennai

ABSTRACT

In the investigation of a crime and the identification of the offenders or the victims, the investigator uses the method called Biometrics for the very accurately confirmation of the both. This Biometrics has come across different stages of its evolution and attained the present stage with the invention and development is the science and technology. Whenever an investigating officer examines a crime scene he first tries to find out the presence of any finger prints. These finger print analysis is one of the oldest methods of using biometrics in the investigation of crime. This was first developed in India in the year 1858. This article gives brief information on the present and future use of biometrics in the investigation of crimes.

Keywords :

Fingerprints were adopted officially in the year 1901 in the world for the first time. The use of Biometrics has grown considerably in the more than a century since then. Biometrics is measurements of physical characteristics of individuals that can be used to verify his or her identity when checked against a known exemplar in a database. Fingerprints are probably the best known biometrics but others include palm prints, facial recognition and Iris recognition. Most of the advances have taken place in the last ten years, driven by enhanced technology and efforts to investigate crime effectively.

There are currently more than six billion people on Earth, and there were another six billion here before the current population over the last 1,00,000 years. With very few exceptions, humans are all basically the same. Yet each is also characteristically unique, and each can be distinguished in many ways from any other person alive today or who ever lived in the last 1,00,000 years.

Human differences are the result of what scientists call "chaotic morphogenesis," a term used to describe the process of random variation in growth and development by which each human becomes physically individualized. This is even true for twins who share DNA for the same physical traits, as some of those traits will be manifested in different ways. That is why, for instance, everyone's fingerprints are unique. The differences go to the other internal organs of our body even our heart. We are as different on the inside as we are on the outside.

The internal organs patterns may be hidden inside, but some unique patterns found in other body parts those on the outside, such as the iris and retina of human eyes, the ridges and valleys of human fingerprints, and even the contours of human ears are different from person to person and can serve as built-in identification tags.

Verification versus Identification

Almost all use of biometrics can be classified into one of two operational areas: verification and identification. The uses most often depicted in the media and movies which relate to verification: an individual registers a biometric, usually a fingerprint, in a database ahead of time, and this biometric then functions like a key or a password that permits the individual to use a bank machine or authorizes the individual to log on to a computer. This is a one-to-one comparison to determine, for example, whether the person claiming to be Mr. Karthick really is Mrs. Karthick.

Most law enforcement applications relate to identification. The biometrics used in this context are by no means limited to fingerprints. For identification, a biometric is obtained, either directly from a person or found at a crime scene, and it is compared to a database of thousands or even millions of other biometrics in search of a match. This is a one-to-many comparison, in which an unknown person's biometric data must be checked, for example, not only against that of Mr. Karthick, but also against that of Mr.Subramani, Mr.Kumuravel, Ms.Ranjana, and many others. The distinction between verification and identification has some important policy considerations for law enforcement.

Fingerprints

The standard biometric for law enforcement has long been, and still is, fingerprints. Indications exist that fingerprints were used as identification tools by people 6,000 years ago in Babylon. In the fourteenth century, the Chinese used footprints, palm prints, and fingerprints to sign important documents such as treaties and contracts.

The first organized approach to finger-prints for identification purposes was made in 1858. The idea that fingerprints could be used as a means of personal identification was first put forward by Sir William Herschel, District Magistrate of Hooghly District, of Bengal province. Later, Dr. Henry Faulds gave the idea of tracing a criminal from the latent prints found at the scene of crime and came to the conclusion that no two fingerprints are alike. Based on the idea of Herschel and Faulds, Sir Francis Galton, the renowned English Scientist established scientifically the basic principles of uniqueness and permanency in Finger Prints. It was then that Sir Edward Richard Henry, the Inspector General of Police, Lower Bengal with the able assistance of two Indian officers namely, Khan Bahadur Azizul Haque and Rai Bahadur Hemchandra Bose, developed a system of classification of fingerprints, thereby discarding the anthropometric system of identification. The first ever Finger Print Bureau in the world was established at Writer's Building at Kolkata in the year 1897.

Sir Francis Gallon in the 1890s devised a fingerprint system, making use of what we now call "minutiae": the major features of a fingerprint. In the late nineteenth century, Galton's contem-

poraries called these characteristics Galton's Details. He gave us the concept of the loops, arches, and whorls in fingerprints. This approach was first adopted in Argentina, and the Galton system is now used in much of the Spanish-speaking world.

Sir Edward R. Henry, a British police official in India in the 1890s, built on Galton's work and created a system of classification based on fingerprint patterns. We now know this as the Henry System. Henry eventually returned to the United Kingdom and became an assistant commissioner of the Metropolitan Police in London. In 1901, he started using the Henry System to classify fingerprints collected by his police agency. The Henry System came to be used in almost all the English-speaking world.

Later in India, The Central Finger Print Bureau (CFPB) came into being in 1955 in Kolkata under the administrative control of the Intelligence Bureau. In 1973 the administrative control was transferred to CBI and it was in July, 1986 that the CFPB was finally placed under the administrative control of the newly formed National Crime Records Bureau and is located at New Delhi.

In the United States, the first systematic collection of fingerprints by a federal authority began at the federal prison in Leavenworth, Kansas, in 1904. Meanwhile, the Saint Louis, Missouri, Police Department began collecting fingerprints at about the same time, making it one of the first police agencies to do so. Upon hearing about the agency's efforts, other police agencies started to send their fingerprints to the Saint Louis Police Department. Eventually, the IACP assumed responsibility for the Saint Louis database.

The IACP later asked the federal Bureau of Investigation (FBI) to take on the management of these growing fingerprint files. That database, as along with the fingerprint files from the federal prison system, became the foundation of the FBI fingerprint files in 1924.

Decades later, the use of computers made possible the establishment of the Automated Fingerprint Identification System (AFIS), which has sometimes been referred to as the Automated Fingerprint Imaging System or Automated Fingerprint Information System. In 1999, the FBI's Integrated AFIS (IAPIS), so named because it pulled a number of functions together in one system, became available online.

Fingerprint databases equivalent to AFIS in other nations had gone online a few years before the FBI's IAFIS. Now, a number of systems around the world are moving to a second generation of automated finger-print systems. The FBI is transitioning to a new system called Next Generation Identification (NGI). The Republic of Ireland just went to its second-generation system. The United Kingdom also has moved ahead with its new system, Identl. The Nether-lands is in the process of moving to a second-generation system as well. Along with increased speed and accuracy, the next generation of AFIS will see increased use of photos, palms, and improved latent functionality.

Fingerprint Enrollment

The law enforcement standard has always been 10 rolled fingerprints for enrollment. Known as the gold standard, 10 fingers rolled provide the most data. A second method of taking fingerprints is a flat impression from a single finger. This is sufficient for agencies that are solely concerned with verification of a specific person's claimed identity. The flat impression used on some countries' travel documents is a good example. A third method of fingerprint enrollment is called slaps. Slaps and flats are often confused, but they are not the same thing. Slaps are four fingers taken together. The distinction among flats, slaps, and 10 rolled prints is where the policy considerations between verification and identification come into play. In the AFTS systems that many states and nations are currently upgrading, law enforcement is often being asked to incorporate the fingerprint records | of an immigration service or a customs service or other agency that is concerned with simply verifying the identities of people entering and exiting a country.

But law enforcement is concerned with far more than mere verification. Law enforcement needs to collect as much data as possible. Law enforcement needs to have a 10 rolled print with all the data it contains. Some border control authorities would rather have a quick flat impression. One can see from their business models why they would want that fast verification. But this is something that law enforcement will have to resist because one characteristic on the side of somebody's finger could very well turn out to be the one piece of evidence that winds up on a piece of paper or on a bomb fragment, suddenly becoming quite important.

The biometric traces left behind on a bomb fragment are referred to as tracing or markings in all the countries except in US. They are called 'latent prints' in the United States. Latents are extremely important. Fingerprints are the only biometric that leaves something behind. And that is why, for the foreseeable future, fingerprints are going to remain law enforcement's most important biometric.

Palm Prints

Palm prints largely fell into disuse after the early days of Sir William Herschel, but their importance is being recognized anew in contemporary policing. About 30 percent of all the latents found at a crime scene are palm prints. One part of the palm that is particularly important is popularly called "the writer's palm" that is, the outside palm. In particular types of crimes, such as kidnappings, extortions, and bank robberies, the writer's palm often makes the case. At a bank robber scene, a single subject with a gun might stand in front of the teller with his gun hand resting with its outer palm on the counter. Especially in older banks with counters made of polished marble, metal, or glass, a clear writer's palm print is often left behind.

Sometimes the bank robbery is what is called "a note job." That is when the bank robber does not show a gun but passes a note to the teller claiming to have a bomb or a gun. The robber often takes a sheet of paper from the supply of deposit slips and writes the note right there in the bank. A good writer's palm print left behind is often located where the note was written. Some agencies only take the flat palm. For all of the above reasons, it is important to encourage the taking of the outer palm as well. Palm prints are part of Australia's National Automated Fingerprint Identification System, recognized as a model system. In the United Kingdom's new Ident1 system, palms are an important component.

Facial Recognition

Facial recognition is a relatively new biometric that is garnering attention. Facial recognition has many advantages, a major one being that it is the only biometric that can routinely be obtained surreptitiously. Therefore, it has value for use in surveillances. Facial recognition is not as accurate as fingerprints at least, not yet but it is becoming increasingly more accurate as new advances in the technology are made. There arc a number of different theories of facial recognition; that is, different algorithms exist that scientists use to measure facial characteristics. Most of these are under copyright. Scientists at universities and in research labs of biometric companies continue to develop new approaches. Each approach works differently, looking at different parts of the face or looking at the face in different ways. Ear shape, for example, is the focus of some facial recognition systems. Ear shape changes very little as we age. Some researchers consider the shape of the ear a separate biometric.

None of these facial recognition systems are 100 percent accurate, but some of them are approaching that level. As various facial recognition algorithms merge, the accuracy of facial recognition will increase. For instance, Cognetic, a company based in Dresden, Germany, has a good facial recognition algorithm. They have partnered with Morpho, a company based in Paris, France, which also has a variety of facial recognition algorithms. These two companies are merging their facial algorithms. Other providers and researchers around the world also will be doing this. As different methodologies merge, the result will be increased accuracy. Reliable applications in this field are not far off.

Iris Recognition
Iris recognition is another biometric of recent interest. The iris is the colored ring around the eye. Like fingerprints, the irises are formed in the womb after conception so that no two people, even twins, have the same iris. Everyone has probably seen a very elderly person, such as a 100-year-old woman, photographed or interviewed on television. Sometimes in a close-up of her face you see her eyes sparkling, and they still look very beautiful. The reason is she has the same irises as she did when she was a 19-year-old young woman. Her skin may have wrinkled with age, but the iris has not changed at all.

The iris can be used for both verification and identification. It is not useful in surveillance because no method yet exists to get close enough to the subject's iris without the subject's consent or cooperation.

Confusion sometimes exists between retina and iris scans. The retina is the rear inner surface of the eyeball. It turns out once again, thanks to chaotic morphogenesis that the patterns of veins and nerves in human retinas are different in each individual. The pattern does not change over time, so the retina too can be used for identification. But it is difficult to work with the retina since it is so far back in the head unlike the iris, which is externally visible. Working with retina identification requires significant cooperation from the subject. It has been used in some places for access control (that is, for verification). The Strategic Air Command of the U.S. Air Force and the U.S. Department of Defense has used it for this purpose, but it is not as easy to use as some other biometrics.

Further Biometric Frontiers
Hand geometry is another biometric. Not to be confused with palm prints or fingerprints, hand geometry deals with the shape of the hand. Like retina patterns, hand geometry is used mainly for access control. At the present time it has very little investigative value to law enforcement. There are many-other biometrics being developed: skin texture, vein patterns, finger geometry, and ear shape as a separate biometric.

Speaker recognition is also a biometric. It should not to be confused with voice recognition, which is not a biometric. Voice recognition is used in devices such as dictating machines and translation machines. Voice recognition recognizes the words. Speaker recognition recognizes the person who is speaking.

Other biometrics are even further away in our future. These are being researched but are not near deployment. These include body odor, body salinity, lips, fingernails, and gait. They may have limited use, but each of these biometrics are currently being researched. It may surprise some people to learn that the growing array of biometrics under study does not include DNA. This is because DNA is not a biometric.

Biometrics can be obtained through observation, albeit with the help of high-tech instruments in some cases, but DNA cannot be observed. In the case of DNA, unlike biometrics, an actual tissue sample is required, and, in contrast to biometrics, this sample cannot now be compared immediately and must be examined by an expert. And although DNA identifications are accurate, they cannot distinguish between identical twins as can true biometrics. As DNA patterns are formed at conception, twins will have the same DNA. But biometrics such as irises and fingerprints are formed in the womb, so even identical twins are distinguishable.

Trends in Biometrics
As biometric technology expands, so do the methods by which a person can be identified and the accuracy with which an identification can be made. Here are five areas in which important trends have begun to emerge:

- Fingerprint identification (to include palm prints) will continue to be the main biometric that law enforcement depends on far into the foreseeable future. Law enforcement will continue to want all the data that can be gathered and must continue to resist pressure from other services for the simple "fast flat."

- Facial recognition is going to have increased investigative use and intelligence use. Unlike fingerprints, however, law enforcement likely will not use facial recognition for evidence in the immediate future.

- Palm prints will see increased investigative use in the immediate future. As the national AFIS databases turn over to their second generation, law enforcement should seize the opportunity to make sure that palm prints are included in the new systems.

- Multimodule, sometimes called biofuse, cataloging is putting two or more biometrics together. The FBI will have multimodule capability in its NGI. In multimodule, for example, the digitized data from both a subject's face and a subject's fingers are stored together on the same disk. When there is a hit on either biometric, the results for both are displayed.

- International cooperation and the recognition of the need for it is a major current trend. Law enforcement agencies need to have the means, the modalities, and the shortcuts to share biometric data with one another. As J. Edgar Hoover once said, "Cooperation is the backbone of law enforcement." That quote is now engraved on the courtyard wall of the FBI Building in Washington, D.C. He said it when he was concerned with federal, state, and local authorities in the United States. Now, all the nations of the free world must talk to one another and exchange data.

Whenever any crime happened, the police take the evidence like fingerprints etc., that were left at the crime scene and they quickly searched their database. The digitalize database help the police to search quickly and with that they can transmit the details of the offender like his photos and other information about him to all the stations around. The offender may be is different makeup but can be confirmed with his biometric signature.

REFERENCES

1. The first use of the word "Biometrics" in this sense appears to have been in 1981 in the New York Time, Merriam-Webster's New Collegiate Dictionary. 11th ed., traces the word back to 1902 in different sense: referring to methods of statistical analysis used by biologists. | 2. "Chaotic morphogenesis" is such an important phrase in biometrics that a greater definition may be necessary. Morphogenesis comes from Greek words morpho (form or shape) and genesis (origin). Chaotic, in this sense, has a very specific mathematical definition: a pattern or state of order with apparent disorder- for example, the irregularities of snowflake (Webster's New Collage Dictionary, 3rd ed.). | 3. Berthold Laufer, "History of the finger-print System," Smithsonian Institution Annual Report (1912), reprinted in The Print 16 (March / April 2000): 1-13, http//www.svsfo.org./ The_Print/ THE _PRINT_VOL_16_ISSUSE_02.pdf 1(accessed February 11, 2011) | 4. Willam J.Herschel, The Origin of Finger- Printing (London, England: Oxford University Press, 1916), http. // galton.org/ finerprints/books/herscel/herschel-1916-origins-lup.pdf (accessed February 11, 2011) | 5. Brian Innes, Body in Question: Exploring the Cutting Edge in Forensic Science (New York, N.Y.: Sterling, 2005) 32-33. | 6. G. S. Sodhi and Jadjeet Kaur, "The Forgotten Indian Pioneers of Fingerprint Science," Current Science 88, no.1 (2005):185-191, http://www.ias.ac.in/currsci/jan102005/185.pdf (accessed February 11, 2011) | 7. Homeland Security: Fingerprint identification Systems," GlobalSecurity, http://www.gobalsecurity.org/ security/system/biometrics-fingerprint.htm (accessed February 11, 2011) | 8. "Integrated Automated Fingerprint Identification Systems," Federal Bureau of Investigation, http://www.fbi.gov/ about-us/cjis/fingerprints_biometrics/iafis/iafis (accessed February 11, 2011) | 9. "Fingerprints and other Biometrics: Next Generation Identification," Federal Bureau of Investigation, http://www.fbi.gov/ about-us/cjis/fingerprints_biometrics/ngi/ngi2 (accessed February 11, 2011) | 10. Shaila K.Dewan, "Elementary, Watson: Scan a Palm, Find a Clue," Technology, The New York Times, November21, 2003, http://www.nytimes.com/ 2003/11/21/ nyregion/elementary-waton –scan- a- palm-find-a-clue-.html(accessed February 11, 2011) | 11. "Fingerprints," Crimtrac, http://www.crimtac.gov.au/ system_projects/Fingerprints.html (accessed February 11, 2011) | 12. The word recognition comes from the Latin words re (again) and cognoscere (to know) (Merriam-Webster's Collegiate Dictionary, 11th ed.) It implies that to recognize somebody, that person must already be in one's data bank. | 13. NAFIS, The Australian AIFS, maintains DNA files alongside its biometric files.

Sara Publishing Academy
Indian Journal Of Applied Research
Journal for All Subjects

Editor,
Indian Journal Of Applied Research
8-A, Banans, Opp. SLU Girls College,
New Congres Bhavan, Paldi, Ahmedabad-380006.
Contact.: +91-9824097643 E-mail : editor@ijar.in

Printed at Unique Offset, Novatsing Rupam Estate, Opp. Abhay Estate, Tavdipura, Shahibaug, Ahmedabad