International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 9 • Issue 2 pp. 28-35 March 2018 - Sept 2018 www.csjournals.com

Association between Biometrics and Forensic Science

[1]Dr. Garima Yadav, [2]Dr. Nikita Yadav, [3]Dr. Sarita Kadian
[1,3]Assistant Professor, Bharati College, University of Delhi
[2]Assistant Professor, Bhagini Nivedita College, University of Delhi

Abstract: Identification? Yes, among many other link "identification" we can say bridges the gap between biometrics and forensic science. Forensic science is the scientific body to identify wrongdoer and at the same time biometrics identify or checks the authentication of person. Biometrics found its ancient natural mate in Forensic. In criminal investigations, traces of video footage from a security camera, a recording of a telephone call, or finger marks left on the crime scene and etc. can be presented as proof at the time of judicial process. After all these advantages of biometrics in forensic there comes a challenge. Yes, challenge! When biometric data from crime scene is acquired in an unconstrained environment or if the subject is uncooperative, the quality of the ensuing biometric data may not be amenable for automated person recognition. In this article, we discuss how biometrics and forensic science are related to each other and then challenging problems. We then present some applications where the principles of biometrics are being successfully leveraged into forensics in order to solve critical problems in the law enforcement domain. We proposed a model in which sensor is put at doorbell to collect the hard biometric traits of visitors.

INTRODUCTION

Biometric recognition, or simply biometrics, refers to the automated recognition of individuals based on their biological and behavioral characteristics **[1]**. Examples of biometric traits that have been successfully used in practical applications include face, fingerprint, palm print, iris, DNA, voice and signature (figure 1).

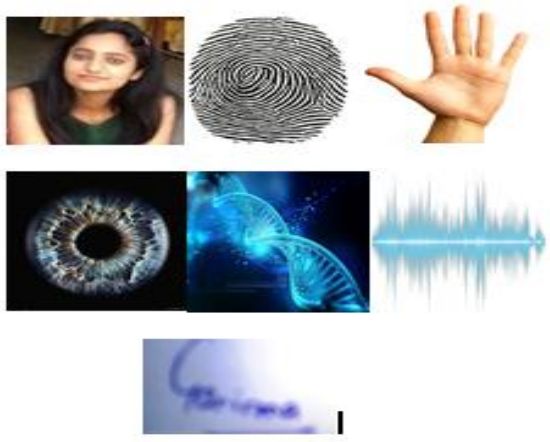

Figure1: Example of various biometric traits

Biometric technology makes a contribution to crime detection by associating the traces to the persons Stored in the database, ranking the identity of persons and selecting subdivision of persons from which the trace may originate**[2].** Biometric traits are inherent to individual and they are unique. Even two same resembling twins have different biometric traits. Biometric system works in four stages. (i)Enrollment Unit: This unit is also called sensor module. It acquires the raw biometric data of an individual in the form of an image, video, audio or some other signal. (ii) Feature Extraction Unit: The feature extraction module operates on the biometric signal and extracts a salient set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user's identity, is stored in the biometric system and is known as a template. (iii) Matching Unit: This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user's master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one too many matching). (iv)Decision Maker: This module accepts or rejects the user based on a security threshold and matching score.**Figure2** below shows the basic structure of biometric authentication system.

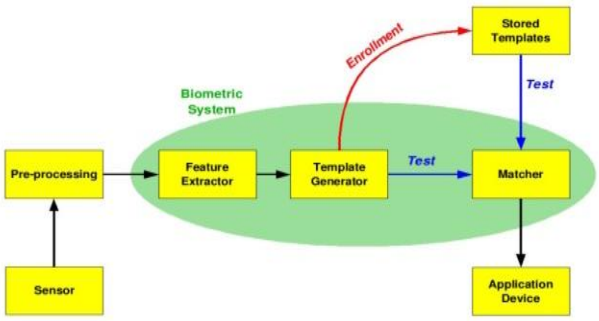

Figure 2: Basic structure of biometric authentication system

Forensic science is the application of scientific principles and techniques to matters of criminal justice especially as relating to the collection, examination, and analysis of physical evidence **[3].** Forensic biometrics uses Fingerprints, palm prints, hand vasculature, hand shape, signature, Face, DNA, sclera (on the eyeball), ear shape and typing patterns (keystroke dynamics), Teeth prints, face, voice, teeth, ear shape and DNA, are also used in forensics.

BIOMETRIC TRAITS USE IN FORENSIC SCIENCE:

Biometric traits are unique to individual and even to similar looking person or twins can't have same biometric traits. So they are very helpful at the time of criminal investigation. Here we will discuss about various biometric traits use in forensic science.

a) FINGERPRINT:

Fingerprints have been used in criminal investigations as a means of identification for centuries. It is one of the most important tools of crime detection because of their robustness and uniqueness. A fingerprint is the pattern of friction ridges and valleys on the surface of a fingertip. In order to match a print, a fingerprint technician digitalizes or scans the print obtained at a crime scene and computer algorithms of a biometric system locate all the unique minutia and ridge points of a questioned print. These unique

feature sets are then matched against a stored fingerprint database. Whenever fingerprints are obtained from the crime scene, they are matched with the fingerprint of near and dears and with the fingerprints of the criminal already enrolled in the database.**Figure3** shows the same.

(a) (b)

Figure3: a) Fingerprint obtained for example from crime scene b) fingerprint from rolled source

b) FACE BIOMETRICS

Biometric face recognition technology plays an important role in law enforcement. Facial recognition is a computer based system that automatically identifies a person on the basis of image or video which is then matched to the facial image stored in a facial biometric database.

c) DNA BIOMETRICS

Deoxyribonucleic acid (DNA), a chain of nucleotides contained in the nucleus of our cells, can be used as a biometric tool to classify and guide the identification of unknown individuals or biological samples left by them. The analysis of the DNA molecule in forensic science is called forensic DNA profiling **[4]**.

DNA of a person can be located throughout his\her entire body. DNA is present in a number of bodily materials such as blood, saliva, hair, teeth, mucus and semen. DNA evidence can be easily found at a crime scene.DNA biometrics uses genetic profiling which is also referred as genetic fingerprinting. In this process the DNA is first extracted from the sample and then segmented into variable number of tandem repeats (VNTR's). These segments are then compared against the stored database.

d) PALMPRINT BIOMETRICS

The palms of the human hands also contain unique pattern of valley and ridges. The area of palm is much larger than the area of a finger, and as a result, palmprints are expected to be even more distinctive than fingerprints **[5]**. Palmprint provides crime investigators an important additional investigative tool. Around 30% of time palm prints are found at a crime scene.

e) IRIS BIOMETRICS

Iris recognition is the automated process of recognizing a person on the basis of unique pattern of iris. The iris is the annular region of the eye bounded by the pupil and sclera (white part of the eye). In the iris recognition, digital templates of iris are compared against the stored templates.

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 9 • Issue 2 pp. 28-35 March 2018 - Sept 2018 www.csjournals.com

f) VOICE BIOMETRICS

Voice biometrics deals with the identification of a speaker from the characteristics of his\her voice. It is often used when voice is the only available trait for identification, e.g. telephoned bomb threat, demand of money in kidnapping cases etc. It has two approaches: Text dependent (recognition based on the fixed predetermined phrases) and text independent (recognition is independent of what a person is speaking).

LINK BETWEEN BIOMETRICS AND FORENSIC:

Biometrics has been used for a long time in forensic science.Forensic science at crime scene at crime scene is deeply influenced by Locard's exchange principle that states that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence **[6].** In his book Crime Investigation: Physical Evidence and the Police Laboratory, Kirk articulates the principle as follows **[7]:**

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool marks he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."

From a long back face, hand writing, threads from the cloth, hairs has been used as the evidence by the forensic Science for the identification of the criminal or the missing person.In year 1892 the first textbook on the biometrics and forensic science was authored by Sir Francis. System of personal identification by bodily measurements developed by French policeman Bertillon became famous. It was known as Bertillon system **[8]**.**Figure3** below shows how various bodily measurement are taken in Bertillon system and use of soft biometric traits for identification from that time.

BERTILLON SYSTEM

Figure3: Bertillon system and use of soft biometric traits.

In Bertillon system many measurements had to be taken from each body part, which was later used for the identification of person. . From about 1910, the fingerprint became more widely used, since it was easy to compare and store in comparison to the Bertillon system, with less error. Face comparison is also commonly done at police stations. The scientific background of face comparisons still should be validated. Iris systems and databases are described to be very effective. However, in forensic science, we do not often get cases with iris-comparisons. In National Geographic, one case is shown where a comparison of a photograph of an Afghan girl with the photograph of a woman gives evidence that they are the same person. The resolution of commonly made digital photographs is not enough to compare the irises. Commercial systems for iris comparison for access control are implemented in airports. The largest database of irises is reported to be in United Arab Emirates, where over half a million irises were in the database in 2005**[9].** DNA databases for criminal cases also exist. In the UK, approximately 4.2 million people or seven percent of the population is in the database in 2006. Compared to Germany and the USA, they only have DNA of 0.5 percent of the population. DNA data is easy to store and not expensive anymore to extract.

In order to find out whether Biometrics and forensic science are linked with each other from a long time or not let's look at few famous cases cracked using biometrics**.[10]**

(i) Ted Bundy(evidence in this case were bite marks of criminal and fibers of victims cloth**)**
Ted Bundy was serial killer responsible for an estimated 30-plus murder, when he was arrested in 1975; there were little physical evidences which prove his crime. Two years later, having been convicted only of kidnapping, Bundy was preparing to stand trial for murder in Colorado when he escaped and headed to Florida. There, he killed three more people early in 1978, and when he was finally captured in February of that year, the physical evidence in those cases led to his conviction. Most crucial was the matching of a bite mark on the buttock of victim Lisa Levy to the Bundy's distinctive, crooked and chipped teeth. He was convicted also of the murder of 12-year-old Kimberly Leach based on fibers found in his van that matched the girl's clothing. Bundy was put to death in 1989.

(ii) The Lindbergh Kidnapping (Biometric evidence in this case was handwriting of kidnapper)

On March 1, 1932, Charles Lindbergh Jr., the 20-month-old son of the famous aviator, was kidnapped, and although a ransom of $50,000 was paid, the child was never returned. Tracking the circulation of the bills used in the ransom payment, authorities were led to Bruno Hauptmann, who was found with over $14,000 of the money in his garage. While Hauptmann claimed that the money belonged to a friend, key testimony from handwriting analysts matched his writing to that on the ransom notes. Additional forensic research connected the wood in Hauptmann's attic to the wood used in the make-shift ladder that the kidnappers built to reach the child's bedroom window. Hauptmann was convicted and executed in 1936.

(iii) The Green River Killer (Biometric data used in this case was the DNA sample)

The Green River Killer was responsible for a rash of murders — at least 48 but possibly close to 90 — along the Green River in Washington state in the '80s and '90s. Most of the killings occurred in 1982-83, and the victims were almost all prostitutes. One of the suspects that police had identified as early as 1983 was Gary Ridgway, a man with a history of frequenting and abusing prostitutes. However, although they collected DNA samples from Ridgway in 1987, the technology available didn't allow them to connect him to the killings. It wasn't until 2001 that new DNA techniques spurred the reexamination of evidence that incriminated Ridgway. He was arrested and later confessed. Ridgway pleaded guilty to 48 murders

— later confessing to even more, which remain unconfirmed — in exchange for being spared the death penalty. He was sentenced to 48 life sentences without the possibility of parole.

There are so many of cases from early 80's till present where biometric used with forensic science and help in the true or correct identification of the wrongdoer. With the advancement in technology day by day criminals are using new tricks for conducting the crime.Therefore,accurate and efficient identification have become a vital requirement for forensic application due to diversities of criminal activities. A recent advancement in biometric technologywhich is equipped with computational intelligence techniques is replacing manual identification approaches in forensic science.

HETEROGENEITY BETWEEN BIOMETRICS AND FORENSIC SCIENCE

Biometrics and forensic science together makes a wonderful team in investigation of crime. In spite of having so many similarities and advantages between biometrics and forensic science, there are lots of difference between the biometrics and forensic science.

a) Different work approaches:

Biometrics and Forensic science works on different approaches. Forensic science works after the occurrence of an event and is typically used to reconstruct past criminal events by a hypothetico-deductive approach. On the other hand, Biometric recognition is typically used before the occurrence of an event.

b) Evidence:

In forensic science investigation of crime scene, no one knows the type of evidence is left by the wrongdoer. It is known after a careful investigation of crime scene. But its opposite in case of Biometric system, in biometric system user knows the biometric trait he/she have to use for their recognition.

c) Real time recognition:

Recognition decisions in biometric systems have to be rendered in *real time* and, therefore, computational efficiency is an important factor in biometric applications. In forensics, however, real-time recognition is not a requirement.

d) Inconclusive decision:

An inconclusive decision in forensics means that crime-scene evidence cannot be associated with certainty to a particular individual. But a biometric system can acquire additional samples of a biometric trait (or of additional traits) from an individual for rendering a 'match' or 'no match' decision**.[11]**

e) Quality:

The quality of the evidence data obtained in the case of forensics is typically lower than that of biometrics. Trace or impression evidence used in forensic investigations has to be meticulously extracted

from a crime scene where, unlike in biometrics, a person does not deliberately deposit the biological evidence. This is one reason why a fully automated scheme cannot always be used to establish a match in the case of forensics.

BIOMETRICS IN YOUR DOORBELL

Now, Biometrics is mature enough to solve most of the criminal cases. But with the advancement in technology criminal cases are increasing day by day. If we say that outsiders or unknown persons are always responsible or commit crime. If you think so, then we might say that you are wrong at hat point.

If we look at criminal cases we will find that offender in most of the cases are the known.There are no common rules that can be used to all of the people, who are involved in crime itself (e.g. offender) or investigation process (e.g. witness). So, it's really very important to be alert all the time but being alert alone is not enough. Here, Biometrics could be helpful. Now, we proposed a model which implements biometric system at doorbell, which automatically collects the finger prints and soft biometric traits(Soft biometric traits are defined as "those characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals" **[12]**. These traits include gender, ethnicity, and color of eye/skin/hair, height, weight, and SMT (scars, marks, and tattoos). It has been noticed thatsoft biometric trait when combined with hard biometric traits (e.g., fingerprint, face, iris, palm vein, etc.) helps in better identification of person) of the person who rings the bell. In this system, we will affix a sensor at the door bell which will scan the fingerprint of visitor and store in the database at the same time camera at the bell collect all the soft biometric traits of visitors. The best of this system is will collect the biometric data of good quality and it will not trouble the visitor.**Figure4** below shows the sensor at doorbell to collect the fingerprints of visitors.

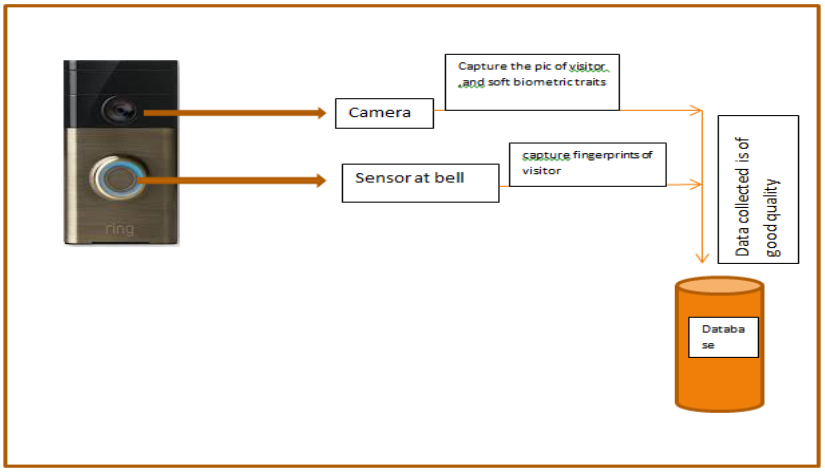

Fig 4: Sensor at doorbell to collect fingerprint of visitor

CHALLENGES WITH PROPOSED SYSTEM:

Implementing this system is not that easy at it seems. Few of the problems which would be faced during implementing this system will be:

a) We need camera of high resolution.

b) We need to maintain the database.

c) Sensor at doorbell can be breakdown with dust.

d) Cost of implementing this system would be high.

CONCLUSION:

In this paper we tried to affix sensor at the doorbell which collect the fingerprint of visitor and camera at doorbell collect the image of visitors. That means at the same time are collecting the hard biometric traits(fingerprint)of visitors and soft biometric traits(color of cloth, hair color and etc) and it has been seen that soft and hard biometric traits together helps in better identification of visitors.

REFERENCES:

1. Jain AK, Ross A, Nandakumar K. 2011 Introduction to biometrics: a textbook. Berlin, Germany: Springer.
2. Jain AK, Patrick Flynn, Arun AR (2007) Handbook of biometrics. Springer,
3. https://www.merriam-webster.com/medical/forensic%20science
4. Dessimoz D and Champod C (2008) Linkages between biometrics and forensic science. In: Handbook of biometrics. Springer, US.
5. Zhang D, Kong WK, You J, et al. (2003) Onlinepalmprint identification. Pattern Analysis and Machine Intelligence, IEEE Transactions 25: 1041-1050.
6. http://rstb.royalsocietypublishing.org/content/370/1674/20140254
7. Kirk P. 1953 *Crime investigation: physical evidence and the police laboratory*. New York, NY: John Wiley & Sons.
8. Bertillon A. 1896 Signaletic instructions including the theory and practice of anthropometrical identification. (Transl. McClaughry RW). New York, NY: The Werner Company.
9. http://www.fidis.net/resources/fidis-deliverables/hightechid/int-d37001/doc/27/
10. http://www.criminaljusticeschools.org/blog/10-famous-cases-cracked-by-forensics/
11. http://rstb.royalsocietypublishing.org/content/370/1674/20140254
12. Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security – Sowmya, Suryavara, Shuchita Kapoor, Shweta Dhatterwal, RohailaNaaz and Anand Sharma, Modi Institute of Technology and Science, Lakshmangarh, Rajasthan, India- 2011 International Conference on Information and Network Technology IPCSIT vol.4 (2011) IACSIT Press, Singapore.