Journal of Forensic Medicine

Saini and Kapoor, J Forensic Med 2016, 1:2
DOI: 10.4172/2472-1026.1000108

Review Article Open Access

Biometrics in Forensic Identification: Applications and Challenges

Monika Saini* **and Anup Kumar Kapoor**

University of Delhi, Delhi, India

***Corresponding author:** Monika Saini, University of Delhi, Delhi, India, Tel: 91-8130634711; E-mail: mini.1901@yahoo.com

Rec date: March 04, 2016; **Acc date:** May 19, 2016; **Pub date:** May 25, 2016

Abstract

Accurate and efficient identification have become a vital requirement for forensic application due to diversities of criminal activities. A recent advancement in biometric technology which is equipped with computational intelligence techniques is replacing manual identification approaches in forensic science. Biometrics is a fundamental verification mechanism that identifies individuals on the basis of their physiological and behavioral features. These biometric expansions are easily observable in different forensic identification areas, e.g. face, fingerprint, iris, voice, handwriting, etc. The effectiveness of biometrics system lies in different recognition processes which include feature extraction, feature robustness and feature matching. The emergence of forensic biometrics covers a wide range of applications for physical and cybercrime detection. Forensic Biometrics also overcomes the loopholes of traditional identification system that were based on personal probabilities. It is considered as a fundamental shift in the way criminals are detected. The present study describes the contribution and limitations of biometric science in the field of forensic identification.

Keywords: Forensic science; Manual identification; Biometrics; Computational intelligence; Forensic biometrics; Criminal identification

Crime and Forensic Science: A Linkage

The extent of reported crime incidents is increasing perilously day by day. Crime is an intentional act or omission in violation of criminal law, committed without defense or justification, and sanctioned by the state as a felony or misdemeanor. It is a deviation from social norms administered by law and its type of costs adversely affects everyone in a society to some extent. Therefore, there is an acute need of accurate and efficient crime detection that may assist in fighting wide verities of criminal activities.

Forensics techniques are being used in the investigation of criminal activities as traditional methods. "Forensic science" begins with the effective identification, documentation (collection of notes, photographs, sketching and videos of crime scene), collection and preservation of physical (covers items of non-living origin such as fingerprints, footprints, fibers, paint, tire or shoe impression and weapons) and biological evidence (originates from a living source and includes DNA, other bodily fluids, hair, skin and bone material) at the crime scene. The evidence is then subjected to scientific analysis in the forensic laboratory and the results of the examinations yield forensic evidence for consideration by court. Ultimately, the evidence will be presented as proof that a crime was committed and will prove the identification of the criminal [1].

A number of methods like forensic anthropometry, forensic dactyloscopy, forensic odontology and forensic document examination are major tools of criminal identification that exist from the end of 19th century. These methods use physical characteristics for the identification or individualization of a criminal.

Limitations of Forensic Science in Criminal Identification

Today, forensic science is facing a number of challenges in the process of crime detection. These challenges are as follows:

Insufficiency of available evidences: The presence of small piece of physical or biological evidences that are hidden in a chaotic crime scene is a type of challenge that is commonly faced by crime investigator. Examples include a small portion of fingerprints, ear print, shoe prints, fraction of dental features, concealed handwriting and unnoticeable paint scratch.

Identity concealment: The majority of criminals devote their knowledge in covering or disguising their activities to conceal their true origin. Therefore, sometimes the human forensic expertise remains inefficient in studying the specific properties of the evidences. For example: Skilled forgeries.

Time consumption: The traditional forensic methods of criminal identification and verification are very time consuming process. The analysis and comparison of crime data against a volume of suspected data is a tedious process.

Lack of standardization: Crime detection is based on the standardized investigative procedures. Due to the limitations of cognitive abilities of human forensic expertise in the case of large volume data, lack of standardization poses a great challenge.

The conventional forensic approach of crime investigation is time-consuming resulting in a lot of delay and often inefficient leading to high expenditure. So there is a need to automize the crime investigation procedure that can give accurate and reliable crime detection results.

Biometrics: A Strong Alternative for Crime Detection

Biometrics is one of the most fascinating ways to solve the crime. It is an automated way to establish the identity of a person on the basis of his or her physical (finger print, face, hand/finger geometry, iris, retina, ear, etc.) and behavioral characteristics (signature, voice, gait, odor, etc.). 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.

A biometric system is a pattern recognition device that acquires physical or behavioral data from an individual, extracts a salient feature set from the data, compares this feature set against the features set stored in the database and provides the result of the comparison. Therefore, a biometric system is composed of four modules [2]:

Sensor module: This component acquires the raw biometric data of an individual by scanning and reading. For example, In case of fingerprint recognition, an optical fingerprint sensor may be used to image the ridge pattern of the fingertip. The quality of raw data is influenced by the scanning or camera device that is used.

Quality assessment and feature extraction module: For further processing, the quality of the acquired raw data is first assessed. The raw data is subjected to signal enhancement algorithm to improve its quality. This data is then processed and a set of salient features extracted to represent the underlying trait. This feature set is stored in the database and is referred as template. For example, the position and orientation of minutia in a fingerprint image is extracted by the feature extraction module in finger print biometric system.

Matching and decision making module: In this module, the extracted templates are then matched against the stored templates and a matching score is given. On the basis of the matching score, the identity of a person is validated or ranked.

System database module: This module acts as storage of biometric system. During the enrolment process, the template extracted from raw biometric data is stored in the database along with some biographic information (such as name, address, etc.) of the user.

Characteristics of Biometrics

The selection of each biometric trait depends on the variety of issues besides its matching criteria. Jain et al. [2] have identified seven factors that determine the suitability of a physical or behavioural trait to be used in biometric application.

1. **Universality:** Every individual who is using the biometric application must possess the trait.

2. **Uniqueness:** The trait must show a sufficient difference across individuals comprising the population.

3. **Permanence:** The given biometric trait should not change significantly over a period of time.

4. **Measurability:** The trait should be easy to get and digitize and should not cause inconvenience to the individual. It should also be amenable to process further in order to extract features from the acquired data.

5. **Performance:** The recognition accuracy and the resources acquired to achieve that accuracy must meet the constraints imposed by the individual.

6. **Acceptability:** Individuals that will access the biometric device should be willing to present their biometric traits to the system.

7. **Circumvention:** It refers to the ease with which the trait of a person can be imitated or copied by using artefacts (e.g. fake fingers in case of physical and mimicry in case of behavioural traits). The biometric system should be immune to the circumvention.

Identification and Verification

Biometrics system can be classified into two main categories on the basis of application mode: Verification and Identification

In the identification mode, the biometric system identifies an individual by searching the templates of all the individuals whose identification details are stored in the database. In this process, the system conducts a one to many comparison to prove the identity of a person.

In the verification mode, the biometrics information of an individual, who claims certain identity, is compared with his own biometric template stored in the system database. This is also referred as one to one comparison.

Biometric technologies find a place in crime detection in a number of ways: (a) The modules and techniques of biometrics help in analyzing the evidence by overcoming the limitations of human cognitive abilities and thus increases efficiency and effectiveness of investigation (b) These methods provide scientific basis (by applying techniques of computer science, applied mathematics and statistics) and standardization for crime investigation procedure by analyzing huge bulk of data which are not humanly possible (c) These techniques provide the advantages of visualizing and documenting the result of analysis.

Development of Biometric technology

The implementation of automated fingerprint identification system (AFIS) in 1960 established the first application of biometrics where the automation of identity verification was based on the ten print cards. In 1980's forensic DNA profiling was discovered where identity verification was done on the basis of DNA reference material using a computerized DNA database.

As a consequence of the development of mobile telecommunication and camera surveillance technologies (CCTV), speaker, face and gait recognition became important biometric tools in the 1990. After 2001 the interest rose for soft biometric modalities such as body measurements (height, width, weight) and proportions, gender, hair, skin colour and clothing characteristics. This interest was mainly motivated by the possibility of capturing these features in unconstraint environments [3].

Data Acquisition in Biometric System

In the forensic context, a test sample obtained from a crime scene is referred as crime scene sample, traces material and questioned item whereas the reference sample that is compared against the crime scene sample is named controlled material or known item. Some of the trace samples (biological traces, finger marks, earmarks, bite marks and lip marks) are collected physically while others are acquired digitally (face, voice, body measurements and gait).

The particular biometric trait needs to be unique, distinctive and robust to the forensic conditions. Therefore, finger-marks and biological traces are searched in priority on a crime scene. The performance of a biometric system is largely influence by the quality of input sample conditioned by the acquisition and environmental conditions of a crime scene.

Applications of Biometrics in Forensic Investigation

Fingerprint biometrics

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.

The Integrated Automated Fingerprint Identification System (IAFIS) is a national automated fingerprint identification and criminal history system maintained by the Federal Bureau of Investigation (FBI). IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

IAFIS houses the fingerprints and criminal histories of 70 million subjects in the criminal master file, 31 million civil prints and fingerprints from 73,000 known and suspected terrorists processed by the U.S. or by international law enforcement agencies.

The average response time for an electronic criminal fingerprint submission is about 27 min, while electronic civil submissions are processed within an hour and 12 min. IAFIS processed more than 61 million ten-print submissions during Fiscal Year 2010.

In September 2014, the FBI announced that its Next Generation Identification system was at full operational capability and effectively replaced IAFIS.

The Ministry of Home Affairs, Government of India is also going to set up a national fingerprint database of 28 lakh convicts to enable speedy identification of offenders and expedite ongoing probes.

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.

In 2012 the FBI launched the Interstate Photo System Facial Recognition Pilot project in three states, and as of June 2014 the system was fully deployed. It allows participating law enforcement organizations to use face recognition to search against more than 15 million mug shots, returning a ranked list of potential matches by using algorithms to search for a match.

The system matches the photo taken at the booking station or from a crime scene with mug shots in the NGI (Next Generation Database) database that have a high probability of being a match. The Michigan State Police have found facial recognition to be very beneficial in attempting to identify unknown subjects who commit crimes of identity theft and fraud [4].

In October, 2001, Fresno Yosemite International (FYI) airport in California deployed Viisage's face recognition technology for airport security purposes. The system is designed to alert FYI's airport public safety officers whenever an individual matching the appearance of a known terrorist suspect enters the airport's security checkpoint [5].

UK-based company NEC IT Solutions, which also specializes in identification of terrorists and criminals, has created a system that analyzes the faces of potential customers as they enter shops. The system then checks this information against a database with celebrities and valued customers - to help stores identify potential big spenders [6].

NEC's NeoFace Reveal is a latent face workstation that reduces investigation time for cases that contain facial video evidence, thus reducing case load for investigators. Another advantage of NeoFace Reveal is its rapid processing of facial evidence coupled with its ability to generate persons of interest list investigation immediately after the crime has taken place.

This advantage allows investigators identify a suspect prior to the suspect evading capture by leaving the local community, state or country [7].

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 [8].

The use of DNA (Deoxyribose nucleic acid) in crime investigation has grown in recent years. It helped law enforcement in a great way to identify the criminals and solve difficult crimes.

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.

The federal Bureau of Investigation (FBI) in 1990 launched a national DNA database, CODIS (Combined DNA Index System) which can be used to identify possible suspects by matching DNA profiles. This database is assisting in forensic crime laboratories at the local, state and federal levels to identify criminals and solve crimes.

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 [9]. Palmprint provides crime investigators an important additional investigative tool. Around 30% of time palm prints are found at a crime scene.

In May 2013, FBI launched a Palmprint database which is assisting crime investigators in positive identification of criminals.

NEC and PRINTRAK companies have developed several palmprint identification systems for criminal application. In these systems high resolution palmprint images are captured and then detailed features like minutiae are extracted for matching the latent prints [10].

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.

The federal Bureau of Investigation (FBI) planned a database for searching iris scans nationwide to more quickly track criminals.

The UK government in 2002 began IRIS (Iris recognition immigration system) program which enables more than a million registered travelers to enter the country via several British airports using only automatic iris recognition for identification, in lieu of passport presentation or any other means of asserting an identity.

Iris recognition system are also used in providing positive identity assurance for larger transactions at live teller stations which lower the risk of losses due to identity theft.

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).

AGNITIO's voice ID technology is a voice biometric tool designed for criminal identification experts and scientific police to perform speaker verification. It is used in court in more than 35 countries worldwide. The traits measured in a given voice sample are biological, expressed through the actual sound of a suspect's voice rather than the shape of the words they are saying [11].

Russia's Speech Technology Center, which operates under the name SpeechPro in the United States, has invented "VoiceGrid Nation," a system that uses advanced algorithms to match identities to voices.

It enables authorities to build up a huge database containing up to several million voices—of known criminals, persons of interest, or people on a watch list. It takes just five seconds to scan through 10,000 voices, and so long as the recording is decent quality and more than 15 seconds in length. This technique has already been deployed across Mexico [12].

New Emerging Biometric Technologies

Gait biometrics

Gait refers to the peculiar way one walks and it is a complex spatio-temporal biometrics. It can be used to identify a person from a distant point. Therefore, this biometric is appropriate in surveillance scenario where the identity of a person can be surreptitiously established. Recognition based on gait is one of the newer biometrics and needs to be researched in detail.

Gait is a behavioural biometric and influenced by a number of factors such as body weight, walking surface, footwear, nature of clothing, etc.

Keystroke biometrics

It is believed that each individual types on a keyboard in a unique way. This biometric is also not very distinctive and unique in identification but assists in recognition of an individual by offering sufficient discriminatory information.

Keystroke pattern is also influenced by emotional state, keyboard position, type of keyboard etc. Advantage of using keystroke behaviour for recognition is that it can be easily observed unobtrusively as that person is keying the information.

This biometric permits "continuous verification" of an individual's identity over a session after the person logs in using a stronger biometric such as fingerprint or iris.

Odour biometrics

Each object spreads around an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. This would be done with an array of chemical sensors, each sensitive to a certain group of compounds. Deodorants and perfumes could lower the distinctiveness [13].

In addition to these biometric technologies, a number of other biometric modalities such as ear, dental, hand geometry and handwriting biometrics are also used by law enforcement agencies and government sectors to address various identity issues and criminal activities. In some criminal cases, it is also important to identify the ethnicity to which the criminal belongs.

A research has also been done on ethnicity estimation from handwriting patterns [14]. These biometric traits are not very distinctive and unique so they are not used in large scale identification. These technologies assist other major biometric traits to improve the performance of the identification.

It is obvious that no single biometric is the "ultimate" recognition tool and the choice depends on the application. A brief comparison of the above techniques is provided in Table 1 [15].

Limitations of Biometric Systems

Due to different positioning on the acquiring sensor, imperfect imaging conditions, environmental changes, deformations, noise and bad user's interaction with the sensor, it is impossible that two samples of the same biometric characteristic, acquired in different sessions, exactly coincide.

For this reason a biometric matching systems' response is typically a matching score s (normally a single number) that quantifies the similarity between the input and the database template representations. The higher the score, the more are the chances that two samples will coincide.

Biometric Characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
DNA	H	H	H	L	H	L	L
Palmprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Voice	M	L	L	M	L	H	H
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odour	H	H	H	L	L	M	M

Table 1: A Comparison of various biometric technologies

A similarity score s is compared with an acceptance threshold t and if s is greater than or equal to t compared samples belong to a same person. Pairs of biometric samples generating scores lower than t belongs to a different person. The distribution of scores generated from pairs of samples from different persons is called an impostor distribution, and the score distribution generated from pairs of samples of the same person is called a genuine distribution [16] (Figure 1).

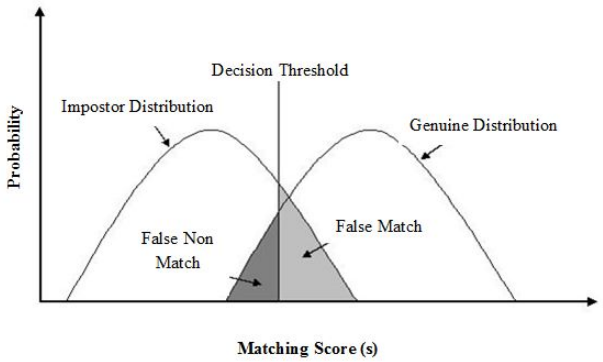

Figure 1: Biometric system error rates.

The main system errors are usually measured in terms of

FNMR (false non-match rate) – mistaking two biometrics measurements from the same person to be from two different persons;

FMR (false match rate) – mistaking biometric measurement from two different persons to be from the same person.

FNMR and FMR are basically functions of the system threshold t: if the system's designers decrease t to make the system more tolerant to input variations and noise, FMR increases. On the other hand, if they raise t to make the system more secure, FNMR increases accordingly [1]. FMR and FNMR are brought together in a receiver operating characteristic (ROC) curve that plots the FMR against FNMR at different thresholds [16] (Figure 2).

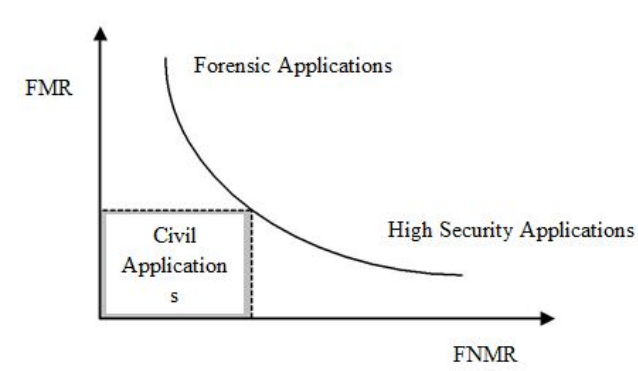

Figure 2: Receiver operating characteristic curve.

There are two other recognition error rates that can be also used and they are: failure to capture (FTC) and failure to enroll (FTE). FTC denotes the percentage of times the biometric device fails to automatically capture a sample when presented with a biometric characteristic. This usually happens when system deals with a signal of insufficient quality. The FTE rate denotes the percentage of times users cannot enroll in the recognition system.

Multimodal Biometrics in Crime Detection

Multimodal biometrics allows the integration of two or more than two biometric recognition and verification systems in order to enhance performance requirements of identification. These systems are more reliable due to the presence of multiple biometric evidences. A multimodal system could be, for instance, a combination of fingerprint verification, face recognition, voice verification and smart-card or any other combination of biometrics. This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric.

The future probably belongs to multimodal biometric systems as they alleviate a few of the problems observed in unimodal biometric systems. Multimodal biometric systems can integrate information at various levels, the most popular one being fusion at the matching score level. Besides improving matching performance, they also address the problem of non-universality and spoofing [13].

Terrorists, smugglers and illegal immigrants gain access in crossing international border by faking their fingers and faces in case of single biometric trait. Therefore, a number of countries like Hong Kong, USA, Japan and Australia are to deploy multimodal biometric border control system that incorporate airline check in with immigration check out.

Conclusion

Accurate and reliable identification is an important issue in crime detection. The biometric recognition is emerging as a sound scientific justifiable tool in investigative procedure. It holds the potential to solve the criminal activities. The augmentation of wide varieties of criminal activities and advances in biometric technology mean that biometrics will have a more marked impact in crime detection in coming future. However many improvements in the recognition systems can be expected if recent findings in applied mathematics, statistics and computer sciences are implemented in biometric science.

Acknowledgement

This work was financially supported by University Grant Commission in the form of senior research fellowship to Monika Saini.

References

1. Fish JT, Miller LS, Braswell MC (2013) Crime scene investigation. Routledge.
2. Jain AK, Patrick Flynn, Arun AR (2007) Handbook of biometrics. Springer.
3. Meuwly D, Veldhuis R (2012) Forensic biometrics: From two communities to one discipline. In: Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the IEEE.
4. Trader J (2014) 5 ways Biometrics help solve crimes.
5. Parmar DN, Mehta BB (2014) Face Recognition Methods and Applications.
6. Stenman J (2013) Embracing big brother: How facial recognition could help fight crime. CNN.
7. NEC Corporation of America (2013) NeoFace® reveal advanced criminal investigative solution using face recognition technology.
8. Dessimoz D, Champod C (2008) Linkages between biometrics and forensic science. In: Handbook of biometrics. Springer, US.
9. Zhang D, Kong WK, You J (2003) Online palmprint identification-Pattern Analysis and Machine Intelligence. IEEE Transactions 25: 1041-1050.
10. (2003) NEC automatic palmprint identification system.
11. Counter PB (2015) Invisible Biometrics Month: 4 Unique Applications of Voice Biometrics.
12. Gallagher R (2012) Watch your tongue: Law enforcement speech recognition system stores millions of voices.
13. Delac K, Grgic M (2004) A survey of biometric recognition methods. In: Electronics in Marine. Proceedings Elmar 2004. 46th International Symposium. IEEE.
14. Saini M, Kapoor AK (2014) Estimation of ethnicity from handwriting patterns. Everyman's Science 20-23.
15. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. Circuits and Systems for Video Technology. IEEE Transactions 14: 4-20.
16. Prabhakar S, Pankanti S, Jain AK (2003) Biometric recognition: Security and privacy concerns. IEEE Security and Privacy 33-42.