International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.04, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A STUDY ON THE APPLICATIONS OF BIOMETRICS IN FORENSIC SCIENCE

Mahroosh Banday[1], A.H.Mir[2]

[1,2]Department of Electronics and Communication Engineering,
National Institute of Technology, Srinagar, India

ABSTRACT

Biometrics is a rapidly developing and yet emerging field of technology, with immense potential, which helps to make our lives easier and safer. Biometrics is widely used in many areas such as security monitoring, database access, forensic applications, and for verification and identification. Accurate and efficient identification have become a vital requirement for forensic application due to increasing criminal activities. Identification approaches in forensic science are being replaced by recent advancement in the biometric technology which is equipped with computational intelligence techniques. Almost all biometric modalities like, face, fingerprint, iris, denture etc. are used in different forensic identification areas. The emergence of forensic biometrics covers a wide range of applications which include identification of criminals, mass disaster victim identification, and identification of fire victims etc. Forensic Biometrics also overcomes the loopholes in traditional forensic identification systems that used manual ways for person identification. It is considered as a fundamental shift in the way criminals were detected. The study in this paper describes the contribution and limitations of biometrics in the field of forensic science.

Keywords: *Biometrics; Forensic science; Forensic biometrics; Criminal Identification, Disaster Victim Identification.*

1. INTRODUCTION

Recent years have seen an exponential growth in the use of various biometric technologies for trusted automatic recognition [1] of humans in different applications such as security monitoring, surveillance, forensic applications and criminal identification. These systems rely on the evidence of fingerprints, hand geometry, iris, retina, face, hand vein, facial, signature, voice, etc. to either validate or determine an identity. The extent of reported crime incidents are increasing day by day. Crime is an intentional violation [2] 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 varieties of criminal activities

[2, 3]. Moreover, in several circumstances when there is inaccessibility to the conventional biometric features, i.e., iris, fingerprint, dental features can be used in forensics [4] to identify the missing persons, the bodies of victims of violent crimes or motor vehicle accidents where the bodies of the victims could be disfigured to such an extent that identification from conventional modalities is not possible. "Forensic science" begins with the effective identification, documentation and preservation of physical and biological evidence which include fingerprints, footprints, fibers, paint, tire or shoe impression and weapons , teeth, DNA, bodily fluids, hair, skin and bone material found at the crime scene [2] or place of calamity . The evidence is then subjected to scientific analysis in the forensic laboratories which will be presented as forensic evidence for consideration by court that a crime was committed and will prove the identification of the criminal [5,6] or can be used by forensic odontologists to establish the identity of the disaster victims. A number of methods like forensic anthropometry, forensic dactyloscopy, forensic odontology and forensic document examination are major tools of criminal and victim identification. Based on the information provided by experts from the Criminal Justice Information Services Division (CJIS) of the FBI, there are over 100,000 unsolved cases of missing persons in the National Crime Information Center at any given point in time. 60 percent of these cases have remained in the computer system for 90 days or longer [7]. Dental records have been used to identify the victims of disasters, such as the 9/11 terrorist attack [7,8] and the Asian tsunami victims [9]; thus the importance of using dental records for forensic human identification is now well recognized.

Forensic science is facing a number of challenges in the process of identity detection. These challenges are as follows:

1. *Insufficient 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.
2. *Identity concealment:* Sometimes the human forensic expertise remains inefficient in studying the specific properties of the evidences [10]. For example: Skilled forgeries.
3. 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.
4. *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 and victim identification is time consuming resulting in a lot of delay and are very complex leading to high expenditure. Owing to the evolution of information technology and an urge to investigate more cases by the forensic experts, it is necessary to automate the human identification

system and biometrics linked with forensics provides a way-out for the problems associated with manual identification in forensic investigation.

II BIOMETRICS 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 based on a feature vector derived from a specific physiological (finger print, face, hand/finger geometry, iris, retina, ear, etc.) or behavioral characteristic (signature, voice, gait, odor, etc) [11] that the person possesses in order to securely identify them to a computer or other electronic system. 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.

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, teeth, jaw bone and lip marks) are collected physically while others are acquired digitally (face, voice, body measurements and gait). Finger-marks and biological traces are searched in priority on a crime scene. The main Biometric modalities that are used in investigation of crime are:

A. Fingerprint Biometrics

Fingerprints have been used in criminal investigations as a means of identification for centuries 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 endings and bifurcation points of a questioned print. These unique feature sets are then matched against those stored in the fingerprint database.

The Integrated Automated Fingerprint Identification System (IAFIS) is a national automated fingerprint identification and criminal history system maintained by the 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. 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 criminals and terrorists in order to expedite ongoing probes.

B. Face biometrics

Facial recognition is a computer based system that automatically identifies a person on the basis of image or video [12,13] 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. In October, 2001, Fresno Yosemite International (FYI) airport in California deployed Visage's face recognition technology for airport security purposes. The system is designed to alert FYl's airport public safety officers whenever an individual matching the appearance of a known terrorist suspect enters the airport's security checkpoint [10]. NEC's Neo-Face Reveal [14] 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 Neo-Face 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.

C. 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.

D. 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. 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 [15]. Russia's Speech Technology Center, which operates under the name Speech-Pro in the United States, has invented "Voice-Grid 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 [16].

E. 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 [17]. 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 [17].

Biometric modalities like gait, ordour biometrics, and Keystroke dynamics are some of the emerging biometric modalities that can be used for crime detection in future.

3. BIOMETRICS FOR VICTIM IDENTIFICATION

Biometric systems have been deployed in various commercial, civilian and forensic applications as a means of establishing identity[1,2]. These systems rely on the evidence of fingerprints, hand geometry, iris, retina, face, hand vein, facial, signature, voice, etc. to either validate or determine an identity. But in several circumstances when there is inaccessibility to the conventional biometric features, i.e., iris, fingerprint, dental biometrics plays an important role.

Dental Biometrics: Identification of victims of mass disasters, fire accidents, and victims of heinous crimes is difficult because of non availability of conventional biometric modalities. So, a biometric modality that is resistant to early tissue decay and decomposition is important. Dental structures are resistant to early decay and remain invariant over time. So, they can be the best biometric trait for victim identity verification. Dental features can be used to identify the missing persons, the bodies of victims of violent crimes or motor vehicle accidents where the bodies of the victims could be disfigured to such an extent that identification from conventional modalities is not possible[18,19]. Based on the information provided by experts from the Criminal Justice Information Services Division (CJIS) of the FBI, there are over 100,000 unsolved cases of missing persons in the National Crime Information Center at any given point in time. 60 percent of these cases have remained in the computer system for 90 days or longer [20]. Dental records have been used mainly to identify the victims of disasters, such as the 9/11

terrorist attack[7,8] and the Asian tsunami and also for criminal identification [9,21]; thus the importance of using dental records for human identification is now well recognized. Using Dental radiograms as biometric modality are expected to enhance the recognition rate and security manifold as dental features are spoof-proof, can't be mimicked [22] and can also be of great help in forensic applications. In 1997, the Criminal Justice Information Services (CJIS) division of the FBI created a Dental Task Force (DTF) [23] to foster the creation of an Automated Dental Identification System (ADIS). Automating the postmortem identification of deceased individuals based on dental characteristics is receiving increased attention especially with the large number of victims encountered [24].

4. CONCLUSION

The biometric technology is rapidly emerging as a sound scientific tool in investigative procedure. Accurate and efficient identification have become a vital requirement for forensic applications with an urge to solve more and more cases in less time. Identification approaches in forensic science are being replaced by recent advancement in the biometric technology to overcome the loopholes in traditional forensic identification systems that use manual ways for person identification. This paper describes the contribution of biometrics in the field of forensic science and discusses the role of biometrics to investigate the crimes to identify the criminals and also throws light on the use of dental biometrics for mass disaster victim identification where conventional biometric modalities may not be available for identification.

REFERENCES

[1] Jain .A.K., Patrick. F., Arun. A.R., *'Handbook of biometrics',* Springer, 2007.

[2] Fish. J.T., Miller. L.S., Braswell. M. C, '*Crime scene investigation'*, Routledge, 2013.

[3] Dessimoz. D., Champod. C., 'Linkages between biometrics and forensic science', *in Handbook of biometrics. Springer, US*, 2008.

[4] David, R.S., Paul, G.S.: 'Forensic Dentistry',CRC Press, 2010.

[5] Meuwly. D., Veldhuis. R., 'Forensic biometrics: From two communities to one discipline', *in Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the IEEE*, 2012.

[6] Trader. J., '*5 ways Biometrics help solve crimes'*, 2014.

[7] 'Forensic Identification of 9/11 Victims Ends', http://abcnews.go.com/WNT/story?id=525937&page=1, Feb, 2005.

[8] Shaughnessy, P.O.: 'More than Half of Victims idd', http://9/11research.wtc7.net/cache/planes/evidence/dailynews_halfvictimsidd.html, New York Daily News, Sept, 2002.

[9] 'Dental records beat DNA in tsunami Ids', 'NewScientist.com, news service', http://environment.newscientist.com/chan/earth/tsunami/mg18725163.900-dental-records beat-dna-in-tsunami-ids.html, September 2005.

[10] Prabhakar .S., Pankanti. S., Jain. A.K., 'Biometric recognition: Security and privacy concerns'. *IEEE Security and Privacy* , 2003, pp. 33-42.

[11] 'Biometrics', https://en.wikipedia.org/wiki/Biometrics.

[12] Parmar .D.N., Mehta. B.B., 'Face Recognition Methods and Applications', 2014

[13] Stenman . J., 'Embracing big brother: How facial recognition could help fight crime', *CNN,* 2013.

[14] NEC Corporation of America (2013) NeoFace® reveal advanced criminal investigative solution using face recognition technology.

[15] Counter. P.B., '*Invisible Biometrics Month: 4 Unique Applications of Voice Biometrics',* 2015.

[16] Gallagher. R., '*Watch your tongue: Law enforcement speech recognition system stores millions of voices'*, 2012.

[17] Zhang. D., Kong. W.K., You. J., 'Online palmprint identification', *Pattern Analysis and Machine Intelligence,IEEE Transactions 25:1041-1050*. (2003)

[18] Rehman, F. et al., 'Human identification using dental biometric analysis', *in Proc. Fifth International Conference on DICTAP, IEEE, DOI: 10.1109/DICTAP.2015.7113178, Beirut, Lebanon* , May 2015 , pp. 96-100.

[19] 'National Science and Technology Council (NSTC) Sub-committee on Biometrics', 'Introduction to Biometrics', http://www.biometrics.gov, May 14, 2007.

[20] Jain, A. K., Chen, H., and Minut, S.: 'Dental biometrics: Human identification using dental radiographs', Proc. of 4th AVBPA, IEEE, Guildford, UK, June 2003, pp. 429–437.

[21] Pretty, I. A., Sweet, D.: 'A Look at Forensic Dentistry—Part 1: The Role of Teeth in the Determination of Human Identity', British Dental Journal, Apr. 2001, vol. 190, no.7, pp. 359-366.

[22] Chen, H., Jain, A. K.: 'Dental biometrics: Matching of dental radipgraphs', IEEE Trans. Pattern Anal. Machine Intell. , August, 2005, vol.27,no.8, pp.1319-1326.