Biometrics – An Overview in Forensic Investigation

G.Yashodha
Assistant Professor, Department of Computer Technology,
K.G.College of Arts and Science, Coimbatore
Email: yashosubha@gmail.com

Abstract - Accurate and specialized identification have become a vital prerequisite for forensic application due to diversities of criminal activities. A recent progress in biometric technology which is equipped with computational intellect techniques is replacing manual recognition approaches in forensic science. Biometrics is a primary 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 preprocessing, feature extraction and feature matching. The emergence of forensic biometrics covers a extensive 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 basic shift in the way criminals are detected. The present study describes the contribution and restrictions of biometric science in the field of forensic identification.

Index Terms - Forensic science; Manual identification; Biometrics; Computational intellect; Forensic biometrics; Criminal Identification.

1. INTRODUCTION

Criminal Investigation and Forensic Science: A Relation

The extent of reported crime incidents is increasing hazardously 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 lawbreaking or offense. It is a deviation from social norms administered by law and its type of costs harmfully affects each person 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 conventional 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, 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 picture is associate degree artifact that depicts or records perception, as an example a two-dimensional image, that includes a similar look to some subject sometimes a entity or an individual, therefore providing an outline of it. pictures is also

two dimensional, like a photograph, screen show, and similarly as a three-dimensional, like a sculpture or photograph. They will be captured by optical devices like cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, like the human eye or water surfaces. The subsequent area unit the categories of pictures: volatile image, mental and still image. [12]

1.1 *Drawbacks of Forensic Science in Criminal Identification*

In day today life, forensic science is facing a numerous challenges in the process of crime detection. These challenges are as follows:

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

Identity camouflage: The majority of criminals devote their knowledge in wrapping or disguising their activities to hide their true origin. Sometimes the human forensic expertise relics inefficient in studying the specific component of the evidences. For example: Skilled forgeries.

International Journal of Research in Advent Technology, Vol.5, No.11, November 2017
E-ISSN: 2321-9637
Available online at www.ijrat.org

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

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

So there is a need to automize the crime investigation procedure that can give accurate and reliable crime detection results.

2.BIOMETRICS: A STURDY ALTERNATIVE FOR CRIME DETECTION

Biometrics is one of the most attractive ways to solve the crime. It is an automated way to set up 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 identification 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. Different types of biometrics used in daily life are shown in figure 1. 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. 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.

Feature extraction module: For further processing, the eminence of the acquired raw data is initially 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. 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.

3.DEVELOPMENT OF BIOMETRIC TECHNOLOGY

The accomplishment 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 2001the 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]

Fig 1. Different Types of Biometrics
(www.ieeecomputersociety.org)

4.DATA ACQUISITION IN BIOMETRIC SYSTEM

In the forensic circumstance, a test sample collected 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 manually 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.

International Journal of Research in Advent Technology, Vol.5, No.11, November 2017
E-ISSN: 2321-9637
Available online at www.ijrat.org

5.APPLICATIONS OF BIOMETRICS IN FORENSIC INVESTIGATION

5.1 *Fingerprint biometrics*

Fingerprints have been used in criminal investigations as a means of identification for centuries. It is one of the most significant tools of crime detection because of their stoutness and individuality. 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 the print collected at a crime scene and computer algorithms of a biometric system to 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 Federal Bureau of Investigation (FBI) is maintaining Integrated Automated Fingerprint Identification System (IAFIS) which is a national automated fingerprint identification and criminal history system. IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses. 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. 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.

5.2 *Face biometrics*

Biometric face recognition technology plays a significant role in law enforcement. Facial recognition is a computer based system that robotically identifies a person on the basis of image or video which is then harmonized 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 possible 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 likelihood of being a match. [4] 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]

5.3 *Palmprint biometrics*

The palms of the human hands also include sole pattern of valley and ridges. The area of palm is much bigger than the area of a finger, and as a result, palmprints are expected to be even more distinctive than fingerprints. [6] Palmprint provides crime investigators an important supplementary 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. [7][11]

5.4 *Voice biometrics*

Voice biometrics works with the recognition of a speaker from the characteristics of his\her voice. It is seldom used when voice is the only existing 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. [8]

6.NEW EMERGING BIOMETRIC TECHNOLOGIES

6.1 *Gait biometrics*

Gait refers to the peculiar way one walks and it is a complex spatiotemporal 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. [9]

6.2 *Keystroke biometrics*

It is alleged that each individual types on a keyboard in a distinctive 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 behavior for recognition is that it can be easily

International Journal of Research in Advent Technology, Vol.5, No.11, November 2017
E-ISSN: 2321-9637
Available online at www.ijrat.org

observed unobtrusively as that person is keying the information. [10]

7. MULTIMODAL BIOMETRICS IN CRIME DETECTION

Multimodal biometrics allows the incorporation of two or more than two biometric recognition and verification systems in order to improve performance necessities of identification. These systems are more reliable due to the presence of multiple biometric evidences. A multimodal biometric system could be, for example, a blend of fingerprint and face 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. [12]

8. CONCLUSION

Accurate and reliable identification is an important concern in crime detection. The biometric recognition is emerging as a novel scientific justifiable tool in investigative procedure. It holds the potential to solve the criminal activities. The escalation of wide varieties of criminal activities and advances in biometric technology mean that biometrics will have a more marked impact in crime detection in forthcoming future. However many improvements in the recognition systems can be expected if recent findings is applied.

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,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]Zhang D, Kong WK; You J(2003):Online palmprint identification, Pattern Analysis and Machine Intelligence.
[7]NEC automatic palmprint identification system 2003.
[8]Counter PB (2015):Invisible Biometrics Month: 4 Unique Applications of Voice Biometrics.
[9]Delac K,;Grgic M(2004):A survey of biometric recognition method, Proceedings Elmar.
[10] Saini M; Kapoor AK (2014):Estimation of ethnicity from handwriting patterns, Everyman's Science.
[11]Yashodha G; Bremananth R (2017):An Efficient Feature Extraction Technique for palm-print recognition system,International Journal of Biomedical Engineering and Technology,25,(2-4).
[12]Jain AK;, Ross A; Prabhakar S (2014):An introduction to biometric recognition, Circuits and Systems for Video Technology.
[13].Gokilavani A (2017):Image Compression: Huffman and LZW Techniques, International Journal for Research in Applied Science & Engineering Technology,5(10).