INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2834 - 2841
RECEIVED : 25.02.2018 PUBLISHED : 21.03.2018

APPLICATIONS OF BIOMETRICS IN FORENSIC SCIENCE USING COMPUTATIONAL INTELLIGENCE TECHNIQUE

1. C.N.Rajalakshmi Associate Professor/MCA
Ganadipathy Tulsi‟s Jain Engineering College Vellore
2. A.K.Pavithra II Year MCA
Ganadipathy Tulsi‟s Jain Engineering College Vellore
3. R.Priyanga II Year MCA
Ganadipathy Tulsi‟s Jain Engineering College, Vellore
4.G.Saranya II Year MCA
Ganadipathy Tulsi‟s Jain Engineering College, Vellore

Abstract-

Biometric is a technical term of recognizing a person based on physiological or behavioral characteristics. Among the features measured area face, finger prints, hand geometry, hand writing, iris, vein, etc,. Biometric based solutions are able to provide for confidential financial transaction and personal data privacy. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods. Recent Advancement of biometrics technology which is equipped with “COMPUTATIONAL INTELLIGENCE TECHNIQUES”. Forensic biometrics is understood as the human based and automated biometrics methods used to analyze and interpret biometrics data within several forensic applications. The emergence of forensic biometrics covers a wide range of applications for physical and cyber crime detection. Limitations of forensic biometrics in criminal identification includes insufficiency of available evidence, time consumption etc,.The present study describes the contribution and limitations of biometrics science in the fields of forensic identification.

Keywords- Biometrics; forensic science; computational intelligence techniques; applications; criminalidentification.

I. INTRODUCTION

Forensic science is defined as the body of scientific knowledge and technical methods used to solve questions related to criminal, civil and administrative law. Forensic biometrics can be defined as the scientific discipline that makes use of the biometric technologies.Biometric recognition or simply biometric refers to the automated recognition of individuals based on their biological and behavioral characteristics. A typical biometric system can be viewed as a “real-time” automatic pattern matching system that acquires biological data from an individual using a sensor extracts a set of discriminatory features from this data and compares the extracted features set with database.

Some aspects of this technological progress are potentiality interesting for forensic biometrics. Some of the computational intelligence techniques such as ***acquisition, segmentation, quality assessment, feature extraction, matching, multi-biometric systems and privacy*** are used in forensic biometrics.

II. CHARACTERISTICS OF BIOMETRICS

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

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

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

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

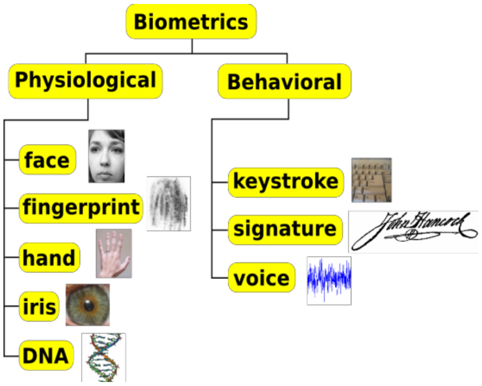
D. ***Measurability*****:** The trait should be easy to get and digitize and should not cause inconvenience to the individual. It should also be amenable to process further in order to extract features from the acquired data.

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

F. ***Acceptability*****:** People that will get to the biometric gadget should exhibit their biometric characteristics to the framework.

III. TYPES OF BIOMETRICS

There are two types of biometrics: Behavioral and physical. Behavioral biometrics are used for verification and Physical biometrics are used for either identification or verification.



A. Behavioral Biometrics

1) *Speaker recognition***:** Analyzing vocal behavior.

2) *Signature Dynamics:* Analyzing signature dynamics.

3) *Keystroke:* Measuring the time spacing of typed words.

B. Physical Biometrics

1) *Finger Print***:** Analyzing fingertip patterns.

2) *Facial recognition***:** Measuring facial characteristics.

3) *Hand Geometric***:** Measuring the shape of the hand.

4) *Iris Recognition***:** Analyzing the features of colored ring of the eye.

5) *Vascular Patterns***:** Analyzing vein patterns.

6) *Retinal Scan:* Analyzing blood vessels in the eye.

7) *Bertillon Age***:** measuring body lengths (No longer used).

IV. BIOMETRICS VERSUS FORENSIC SCIENCE

Forensic science involves the use of logical standards to break down proof at a wrongdoing scene keeping in mind the end goal to remake and portray past occasions in a lawful setting. It has been profoundly impacted by Locard's trade rule that expresses that the culprit of a wrongdoing will carry something into the wrongdoing scene and leave with something from it, and that both can be utilized as scientific proof

> Wherever he steps, whatever he touches, whatever he leaves, even unwittingly, will fill in as a noiseless observer against him. His fingerprints or his impressions, as well as his hair, the strands from his garments, the glass he breaks, the instrument marks he leaves, the paint he scratches, the blood or semen he stores or gathers. These and more bear quiet observer against him. This is confirm that does not overlook. It isn't confounded by the fervor existing apart from everything else. It isn't truant since human witnesses are. It is accurate confirmation. Physical confirmation can't lie itself, it can't be entirely truant. Just human inability to discover it, contemplate and comprehend it, can reduce its esteem.

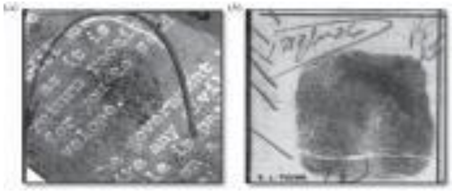


Figure 1

(*a*) The finger mark is an item of evidence retrieved, for example, from a crime scene. (*b*) The rolled fingerprint is obtained from a known source (i.e. known individual).

In this regard, both forensic science and biometric recognition seek to link biological data (impression evidence) to a particular individual. Despite this commonality, there are a number of differences between forensics and biometrics:

(i) Forensic science is **invoked *after*** the occurrence of an event and is typically used to reconstruct past criminal events by a hypothetic-deductive approach. Biometric recognition, on the other hand, is typically **used *before*** the occurrence of an event (e.g. accessing a laptop or entering a country).

(ii) In a forensic investigation it is **not possible to determine in *advance*** the type of evidence that will be used to apprehend the perpetrator of the crime. The crime scene has to be carefully examined in order to glean evidence that is subsequently used for recognition purposes. This is in contrast to biometric systems where the biological traits (i.e. modalities) to be used for person recognition are known **in advance.**

(iii) Forensic science predominantly involves the ***manual*** collection and examination of evidence, compared to biometric recognition which is by definition **fully *automated***.

(iv) **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.

(v) In forensic science, a ***false non-match is highly undesirable*** since it can result in excluding the perpetrator of a crime from further consideration. In the case of biometrics, depending upon the application at hand, the consequences of false matches and false non-matches can be different. For example, in a surveillance system, false non-matches have to be minimized at the risk of increasing false matches; however, in a biometric access control system for a nuclear plant, false matches have to be minimized even if this results in an increased number of false non-matches.

(vi) 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.

(vii) 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.

V. COMPUTATIONAL INTELLIGENCE TECHNIQUES

A. ***Acquisition:*** The acquisition of the biometric sample is the first step in the recognition process, and is performed with the aid of biometric sensors (e.g., optical scanners for fingerprints, digital cameras

B. ***Segmentation*****:** The segmentation step isolates the genuine biometric characteristic from the foundation. This progression is basic to ensure a high acknowledgment rate, and can be affected by numerous components, for example, changes in picture introduction, impediments or shifting light conditions. Furthermore, every characteristic can have particular segmentation challenges. In confront acknowledgment, the segmentation step isolates the face from the foundation, and can be confounded by changes in posture, outward appearance or foundation varieties For the situation of unique mark acknowledgment, the segmentation of the edge design permits to stay away from the extraction of fake highlights from the fo

C. ***Quality Assessmen*****t:** The quality of biometric samples has a great impact on the performance of biometric systems . Quality metrics are then used to predict the recognition performance of a sample, so that higher quality values correspond to a better recognition of the individuals. However, estimating the correspondence between a sample and its recognition capability can be complex. For this reason, CI techniques have been often used in this context to learn the relation between a sample and its quality.

D. ***Enhancement*****:** These techniques have been applied for the enhancement of biometric samples, especially in the case of fingerprint images. In fact, variations in the position and exerted pressure of the finger on the sensor can cause regions of the image where the details of the fingerprint, specifically the ridges and valleys, are not clearly defined. For this reason, a preprocessing step is used to level out the quality of the image before extracting the features.

E. ***Feature Extraction***: The feature extraction process has the purpose of extracting the most distinctive characteristics of the biometric trait, which are then matched in order to perform the identity comparison.

F. ***Matching:*** The matching process compares the features obtained from the live sample with a previously enrolled template, to check if they correspond to the same person. The result of this process is a similarity score. Finally, a threshold is used to determine the acceptance or rejection of the matching. Matching algorithms have to deal with variations of the extracted features, which may appear as a result of changes in the trait (e.g., disease, aging)

G. ***Multibiometric Systems*****:** Multibiometric systems can use multiple acquisition sensors, recognition algorithms, biometric samples, or biometric traits (e.g., face and voice) to enhance the recognition accuracy of biometric systems. Multibiometric technologies present important advantages over traditional biometric systems, such as robustness to problems due to the non-universality of biometric traits (some people cannot use a certain biometric trait), robustness to spoof attacks and noisy data, and increased fault tolerance

Multibiometric systems can perform the information fusion at different levels: sensor-level, feature-level, score-level, rank-level, decision-level.

• ***Sensor-level:*** the raw biometric data are fused to obtain a more discriminative sample and reduce the noise

• ***Feature-level*****:** feature vectors obtained from different feature extraction algorithms are fused to create a single template.

• ***Score-level:*** The match scores obtained by multiple matchers are fused to obtain a single match score.

• ***Rank level*****:** For each matcher, the ranking is computed from a set of all the possible matching identities sorted in decreasing order of confidence

• ***Decision-level***: The final "yes/no" decisions of different matchers are fused. This approach is usually adopted in the cases in which it is not possible to modify existing biometric algorithms to obtain other information.

H. *Classification:* In biometric systems, classification methods are used to partition the set of biometric samples in several classes, so that the matching is performed considering only the samples belonging to the same class, thus reducing the computational time required for the recognition.

I. *Score Normalization*: In the literature, there are studies that aim at increasing the accuracy of biometric systems by post-processing the raw matching scores obtained by the recognition system

VI. APPLICATIONS OF BIOMETRICS IN FORENSIC SCIENCE

A. *Finger Prints*: Finger prints 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.

B. *Face Biometrics*: 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.

C. Iris biometrics: 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: 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 more than 35 countries worldwide.

VII. 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:

A. *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.

B. *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.

C. *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.

D. *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.

VIII. BENEFITS OF BIOMETRICS IN FORENSIC SCIENCE

- Can‟‟t be lent like a physical key (or) token and **cannot be forgotten** like a password.
- Good compromise between **ease of use**, template size, cost and accuracy.
- Biometrics contains enough inherent variability to enable **unique identification** even in very large (millions of records) databases.
- Basically**, lasts forever-** or at least until amputation or dismemberment.
- Makes network login and authentication **effortless.**

CONCLUSION

From an operational perspective this study indicates that the various computational intelligence techniques used in biometrics are very effective in the field of forensic science. Accurate and efficient identification have become vital requirements for forensic applications due to diversities of criminal activities.

In this study, we have discussed the characteristics of biometrics, how the biometrics techniques area applied in the field of forensic science, the challenges on limitations forced by the forensic science departments by using these biometric techniques.

Even though biometric techniques have some limitations. It plays an important role in forensic science.

Hence, these computational intelligence techniques are used to

Identify the criminals by their biometrics and the biometrics is also agreed as evidence in the court of low.

REFERENCE

[1]Umat Uludag, Pankati, Salil Prabakar " Biometric Cryptosystems: Isuues and challenges" Issue:July 2004.

[2]A.K.Jain, R.Bolle and S.Pankanti "Biometrics: Personal Identification in networked society" Norwell M.A.Kluwer 1999.

[3] Massimo Tistarelli, Enrico Grosso and Didser Meuwly " Biometrics in Forensic Science: Challenges, Lessons and New technologies".

[4] Ruggero Donida labati, Angelo Genovere, Enrique Munoz, " Computational Intelligence for Biometric Application: A Survey".

[5]F.Scotti and V.Piuri, "Adaptive Reflection Detection and location in Iris Biometric images by using Computational Intelligence Techniques" IEEE Trans. On Instrumentation and Measurement,Vol.59, No.7, pp.1825-1833,2010.