Building a framework for the development of biometric forensics

Bača Miroslav*, Koruga Petra * Fotak Tomislav*
* Faculty of organization and informatics/Center for Biometrics, Varaždin, Croatia
mbaca@foi.hr; pkoruga@foi.hr; tomislav.fotak@gmail.com

Abstract - Application of biometric tools today is a major challenge for developers of biometric systems and for users of those systems. A specific application can be seen in systems requiring a certain accuracy in person authentication. A large number of systems is created in a way that the algorithms used are not verified as standardized, thus causing uncertainty in their results and application of those tools in processes which need to confirm obtained results. This paper will describe the basic model necessary to build a framework for the construction of a biometric system applicable in forensics for person authentication in court of law.

I. INTRODUCTION

Forensic science is broadly defined as the application of scientific knowledge to the legal system. It includes disciplines like pathology, biometrics, serology, molecular biology, trace evidence and weapons identification[1]. From this definition, it can be seen that one important discipline is biometrics.

Biometrics can be defined as field of technology using automated methods for person authentication using their physiological and behavioral characteristics[2,5]. It can be fingerprint analysis, voice recognition or signature recognition as more common techniques or face recognition, infrared image analysis, palmprint recognition, ear recognition, walk recognition as uncommon techniques.

The use of biometrics in forensics and law enforcement has become common and is used mainly to determine the identity of offenders which is acceptable in court.

This paper will give an introduction to usage of biometrics in forensics and law enforcement. Next, some problems related to biometrics in forensics will be presented and an idea for solution of those problems along with the future research on this topic, will be stated.

II. BIOMETRICS IN FORENSIC SCIENCE

At the time crime is commited, the perpretrator is typically unknown and the investigation has to be conducted in order to find suspects. Biometrics is very usefull in such situations. Especially automated systems for person comparison or identification.

These systems work well for biometric identification or verification, where characteristics are taken in controled conditions, and failure of those systems doesn't have severe consequences. Forensic recognition has severe consequences, because if a systems makes the wrong decision, a person could be convicted and spend time nad jail but be completely innocente.

There are three rules which forensic science must abide[1]:

- Forensic science must apply only those procedures that are solidly grounded through experimentation.
- Standards for qualifying tehnicians and scientists must be followed.
- Standard procedures must be adhered to during evidence collection and analysis.

The more evidence are scientifically grounded, the stronger the case is in court. If methods and technologies are untested, if no standardization exists, if algorithms are misapplied, the case won't stand in court and it is the same as evidence wasn't collected at all.

To this day, a vast number of biometric tools has been developed. The use of those tools in forensic investigations would improve the efficiency of forensic work and standardize the comparison process[3].

Problems with those systems are:

- Results are not robust to changes in, for example, pose or illumination
- Quality of images is usualy bad (taken from a far, low resolution, compression)
- A score based biometric recognition system is not suitable to judicial system where the objective is to give a probability or degree of support for one hypothesis against the other[4]

What makes things easier is that forensic recognition doesn't have to be in real time, so it doesn't have a time constraint.

The most important thing is that the technology in use must be thoroughly tested and evaluated. In European judicial system, there are no admissibility rules regarding scientific evidence[3].

III. BIOMETRIC SYSTEM CHARACTERISTICS

Biometric systems in general have a number of characteristics. Geradts and Ruifrok [6] describe important factors necessary for an effective biometric system:

- Accuracy
- Speed and throughput rate
- Acceptability to users
- Uniqueness
- Resistance to counterfeiting
- Reliability
- Data storage requirements
- Enrollment time
- Intrusiveness of data collection

These characteristics will be described below.

A. Accuracy

Accuracy is the most important characteristic of a biometric system. If the system is not accurate, there is no point to it at all. If a system is for verification (comparison one-to-one) purposes, Geradts and Ruifrok [6] define:

- False Reject Rate (FRR) – percentage at which enrolled person are rejected as unidentified or unverified
- False Acceptance Rate (FAR) – percentage at which impostor persones are accepted as authentic (enrolled) person
- Equal Error Rate (EER) – cross over error rate, stated as a percentage at which false rejection rate and the false acceptance rate are equal (Fig. 1)

For a biometric recognition system Bromba [7] diferentiates between four possibilities:

- Correct match – if two samples of the feature of the same subject match
- False match – If two features of two diferent subjects match
- False non-match – If two samples of the feature of the same subject do not match
- Correct non-match – if two features of two different subjects do not match

B. Speed and throughput rate

Another characteristic important when choosing a biometric system is the speed and throughput rate. The speed of a biometric system is not solely related to the speed or power of the data processing aspect of the system, it relates to the process flow in its entirety - the speed from beginning to end needs to be considered[8]. For example, this means that everything from taking a pen to sign your name to opening and closing the door, if required, should be considered when calculating the speed of the system.

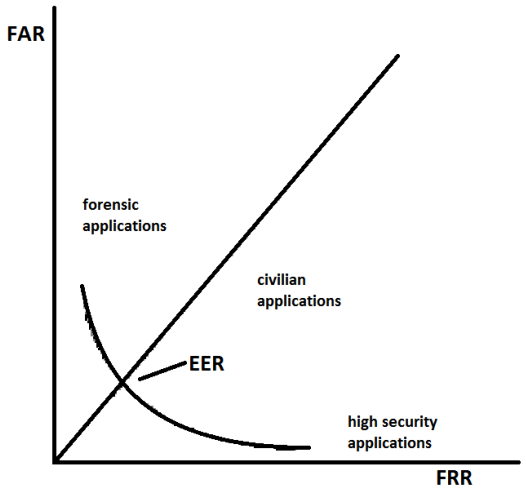

Figure 1. Receiver's Operating Curve: FAR versus FRR[6]

C. Acceptability to users

This is the main concern for users, next to performance. The biometric systems should be intuitive and easy to use. It shouldn't pose any problems to collect characteristics, and users should feel comfortable using it.

User acceptability can be increased in some degree by education and information.

D. Uniqueness of biometric characteristic

The key of every biometric system is the uniqueness of biometric characteristic employed. The most unique are fingerprints which, by now are most commonly used, and iris and retinal scans [8]. Uniqueness does not mean that these characteristics can not be replicated, it just means that they have a sufficient number of complex patterns or traits that can be used to build a strong template for authentication[8].

E. Resistance to counterfeiting

Resistance to counterfeiting is just the question how easily can a characteristic be replicated by an intruder. This is very different from uniqueness. Some characterisics can be very unique, but easily counterfeited.

F. Reliability

Reliability regards downtime of a system. It would be ideal, but impossible, that a system has no downtime. Next demand is for the downtime to be minimal, and when it happens, to be as short as possible. Getting the system back up should be easy with minimal losses of both productivity and data.

G. Data storage requirements

This characteristic may directly influence on speed of the system. If templates used in a biometric systems require are large, speed of processing will be smaller. Also, new hardware may be required[8].

H. Enrollment time

Enrollment is the proces of inputing users in the system. For organizations, it is enrollment of employees. From forensic and law enforcement standpoint, it is enrollment of suspects in the system, or whole country.

Enrollment time may take from several hours to couple of years.

I. Intrusiveness of data collection

Term data collection from this aspect means collection of peoples biometric characteristics (fingerprints, facial images, retina images, iris scans, palmprints, footprints...). Biometric characteristics used in a system should be easy to collect and non-intrusive.

IV. Evaluation Criteria

Simoens [9] in his work on Security and Privacy Challenges with Biometric Solutions gives evaluation criteria for template protection:

- Technical performance
  - Accuracy
  - Accuracy degradation
  - Throughput
    - PI encoding time
    - PI recoding time
    - PI comparison time
  - Storage requirements
    - Protected template size
    - Code size
  - Diversification capacity
- Security and privacy performance
  - Full-leakage irreversibility
  - Authorized-leakage irreversibility
  - Pseudo-authorized-leakage irreversibility
  - Unlinkability
- Operational preformance
  - Modality independence
  - Interoperability
  - Quality of performance
    - Granularity of performance
    - Stability of performance

It is visible that these two different approaches have a lot in common. Accuracy, throughput and storage requirements are visible in both approaches.

Also, in both of those algorithms, two thing important for forensics are missing. Biometric methods and algorithms need to be verifiable and repeatable. Every result obtained by any method must be able to be obtained in the same way, by the same method any time. And if someone knows the result and the method used, this person must be able to verify the given result.

V. Conclusion

Biometric methods are more and more popular in access restriction, but also in forensics and law enforcement. For their proper usage, apropriate standards need to be developed.

This paper points to problems which exist in using biometrics for forensic recognition of individuals in court of law. It describes the characteristics of biometric systems which should be taken into consideration when creating a framework for standardization of biometric methods for forensics purpose esspecially in the court of law. Future work will concentrate on creating a detailed framework for standardization of biometric methods for usage in forensics.

Acknowledgments

Shown results come out from the scientific project Methodology of biometrics characteristics evaluation (016-01611992-1721) financed by the Ministry of Science, Education and Sport, Republic of Croatia.

References

[1] "The National Institute of Justice and Advances in Forensic Science and Technology", National Law Enforcement and Corrections Technology Center, 1998

[2] John D. Woodward, Jr.; Nicholas M. Orlans; Peter T. Higgins: "Biometrics", The McGraw-Hill Companies, 2003

[3] Tauseef Ali; Raymond Veldhuis; Luuk Spreeuwers: "Forensic face recognition:A survey", 2011

[4] Champod, C., and Meuwly, D., “The inference of identity in forensic speaker recognition”, Speech Communication, 31, pp. 193-203, 2000.

[5] Sushil Chauhan; A.S. Arora, Amit Kaul: "A survey of emerging biometric modalities", Procedia Computer Science 2, 2010, 213-218

[6] Zeno Geradts; Arnout Ruifrok: "Extracting forensic evidence from biometric devices", SPIE proceedings Investigative Image processing, 2003

[7] Manfred U. A. Bromba: "Performance Measures for Biometric Recognition", 2010

[8] SANS Institute, InfoSec Reading Room: "Biometrics: An In Depth Examination", 2004

[9] Koen Simoens: Security and privacy Challenges with Biometric Solutions, LSEC Biometrics, 2011