Extracting forensic evidence from biometric devices

Zeno Geradts*, Arnout Ruifrok
Netherlands Forensic Institute, Volmerlaan 17, 2288 GD Rijswijk, Netherlands

ABSTRACT

Over the past few years, both large multinationals and governments have begun to contribute to larger projects on biometric devices. Terrorist attacks in the USA and in other countries have highlighted the need for better identification systems for people as well as improved systems for controlling access to buildings. Another reason for investment in Research and Development in biometric devices, is the massive growth in internet-based systems – whether for e-commerce, e-government or internal processes within organizations. The interface between the system and the user is routinely abused, as people have to remember many complex passwords and handle tokens of various types. In this paper an overview is given of the information that is important to know before an examination of such is systems can be done in a forensic proper way.
In forensic evidence with biometric devices the forensic examiner should consider the possibilities of tampering with the biometric systems or the possibilities of unauthorized access before drawing conclusions.

Keywords: biometrics, forensic, fingerprint, iris

1. INTRODUCTION

With conventional security systems, many users fall prey to socially engineered attacks, or choose easy-to-guess PINs or passwords and then write them down. For reasons of security, biometric systems are used. Systems with fingerprints, iris, hand scans, and face recognition are commercially available and are also used at airports. Many other biometric data is under investigation for commercial systems, as ears, gait, key stroke, odor etc. New developments are in heat maps and thermo-grams, with which developers claim that easier identification of individuals, is possible.

From governments there is an interest to identify persons correctly when they visit a country. An example is the USA which has a Visa-waiver arrangement with many countries. The "Enhanced Border Security and Visa Reform Act of 2001", (S.1479), was agreed by Senate and the House of Representatives easily. The bill requires all foreign travel documents including passports, to contain a biometric feature that can be read by officials at all US ports-of-entry by 26 October 2004. In first instance, the requirement only affect 'aliens' seeking to enter the US under the visa-waiver program if their passports were issued after October 2004[1].

Governments of each visa-waiver country will have to comply if they wish to maintain the visa waiver status. This means that many programs have been started world-wide that issue their nationals with tamper-proof machine readable passports incorporating biometric identifiers that comply with standards established by the International Civil Aviation Organization.

The interest from companies in biometric systems is growing very rapidly, as can be seen in Figure 1, where the number of biometric systems applications is visualized per year. In figure 2, an overview is given of the number of US patent applications for each kind of biometric data for 1997-2002. It appears that most patents are applied for in the area of fingerprints.

- zeno@forensic.to; phone +31704135681; www.forensic.to

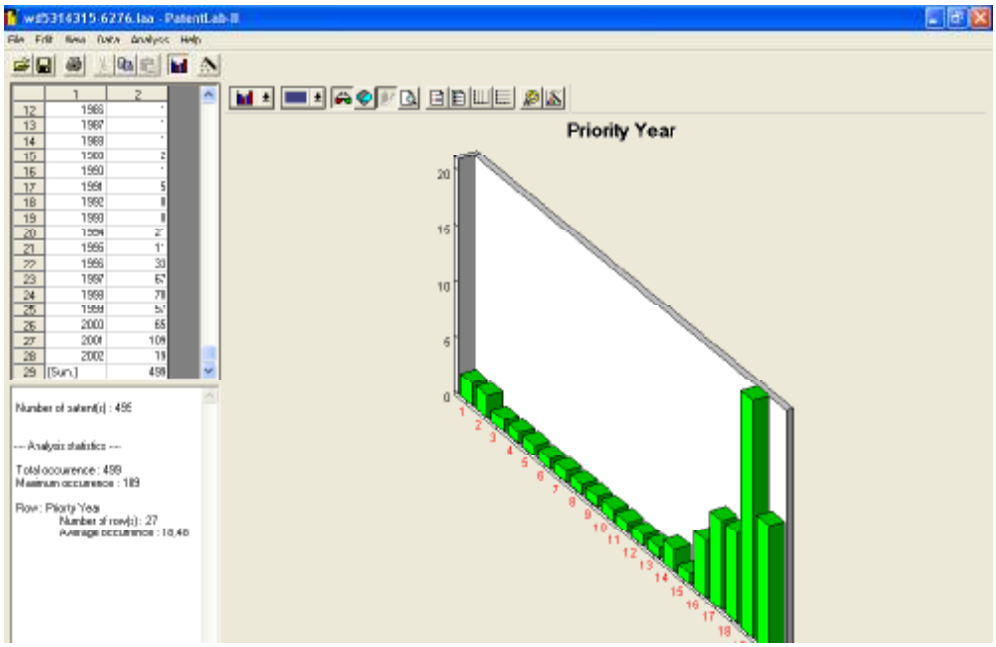

Figure 1 : Number of US Patent Applications per year. Note : the number of applications in 2002 is not completely disclosed in this graph yet..

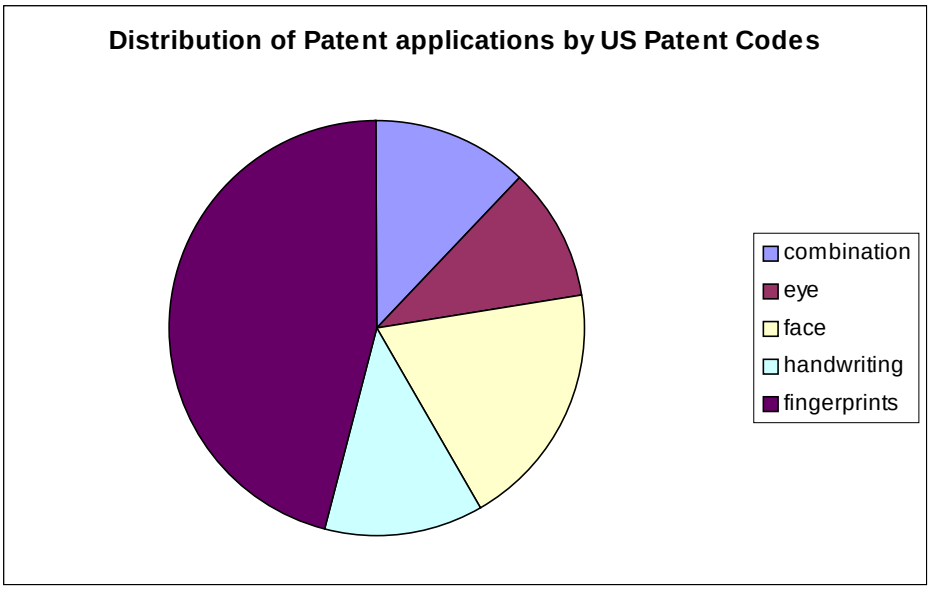

Figure 2 : Percentage of patents applied for from 1997-2002, and the distribution in different biometric data.

Testing and comparison of biometric systems

Testing and comparison of biometric systems is still an issue. Comparison of algorithms used in facial recognition is undertaken in the FERET[2] program, which is followed up by the Face Recognition Vendor Tests[3]. Often of more interest is the "real life" performance in a situation approximating that of future deployment

New suppliers are often tempted to make claims of excellent performance based upon a small laboratory test or mathematical simulations. In practice it appeared that face systems are still not good enough for many applications, since faces change in time, and they are difficult to acquire in a standardized way.

The European BIOTEST project led by the National Physics Laboratory has produced a set of best practice guidelines for these systems that can be used for examining biometric systems. Nowadays we see much effort in standardization, for example the BioAPI[4] Consortium. Standardization committees in many countries are developing standards, an example of this can be found at NIST Biometric Interoperability, Performance, and Assurance Working Group[5]. Another standardization is OASIS, which is developing for internet-based applications in OASIS[6] XML Common Biometric Format (XCBF). The deliverables for this project should be ready at the end of 2003.

New initiatives in the European Union is the BIOVISION[7] consortium, which to develop a roadmap for future biometric developments. Also in the Sixth Framework many new initiatives are expected.

The literature in this field is mostly focused on a well-engineered sensor, or the algorithms that are used. Less well-described are the systems of which biometric is a small part. If it is not integrated securely, or if the system is vulnerable to an unexpected attack, even the best device will be compromised. Often the biometric system compromises a smart card with data of the finger print or the iris scan which is compared with the data of the person that would like to have access.

For forensic evidence the biometric devices can be important, since more information is available of the person who tries to access a building or a computer. In cases with hacking this might also be helpful if a suspect has been logged on with biometric data (e.g. a fingerprint).

With biometric devices it is still possible to have unauthorized access. Depending on the chip card that is used, someone can tamper with the data. Furthermore, it is also possible to copy the data from a person (e.g. with a silicon cast of a finger). The problem with spoofed biometric data is that it can not be revoked and renewed, as would have been done with a stolen key. Another reason for unauthorized access is that there are false acceptance rates, depending on the settings of the biometric device. Often the setting of the biometric device will be changed to have less false rejects, and this might cause the system to fail. In practice. biometrics are not more secure than PINs. For this reason it is good to have a combination of biometric data and PINs or other token (e.g. a chip card) for access.

In forensic evidence with biometric devices the forensic examiner should consider the possibilities of tampering with the biometric systems or the possibilities of unauthorized access before drawing conclusions. This paper shows an overview of possibilities of tampering with these systems, from public available sources.

2. CHARACTERISTICS OF A BIOMETRIC SYSTEM

Important factors necessary for any effective biometric system are [8]:

- accuracy,
- speed and throughput rate,
- acceptability to users,

- uniqueness,
- resistance to counterfeiting,
- reliability,
- data storage requirements,
- enrollment time,
- intrusiveness of data collection

ACCURACY

Accuracy is the most critical characteristic of a biometric system. If the system cannot accurately separate authentic persons from others, it depends on the amount of security that is required if the system is allowed for that use. Most often the systems are for verification (1 to 1 comparison) and not for identification purposes (1 to n comparison).

False Reject Rate (FRR)

The rate, generally stated as a percentage, at which enrolled persons are rejected as unidentified or unverified persons by a biometric system is termed the false reject rate. False rejection is sometimes called a Type I error. In access control, if the requirement is to keep the "bad guys" out, false rejection is considered the least important error. However if used at an airport for access control, it can be very annoying for the passengers if this rate is high.

An associated problem that is sometimes incorrectly attributed to false rejection is failure to acquire. Failure to acquire occurs when the biometric sensor is not presented with sufficient usable data to make an authentic or impostor decision. Examples include smudged prints on a fingerprint system or improper alignment on a iris system.

False Accept Rate (FAR)

The rate, generally stated as a percentage, impostor persons are accepted as authentic, enrolled persons by a biometric system is termed the false accept rate. False acceptance is sometimes called a Type II error. This is often considered to be the most important error for a biometric access control system.

Biometric systems have sensitivity adjustment capability. If false acceptance is not desired, the system can be set to require nearly perfect matches of enrollment data and input data. If tested in this configuration, the system can be stated to achieve a near zero false accept rate. If false rejection is not desired, this system can be readjusted to accept input data that only approximate a match with enrollment data. If tested in this configuration, the system can be truthfully stated to achieve a near zero false rejection rate. The reality is that biometric systems can operate on only one sensitivity setting at a time.

The reality is also that when system sensitivity is set to minimize false acceptance, closely matching data will be spurned, and the false rejection rate will go up significantly. Conversely, when system sensitivity is set to minimize false rejects, the false acceptance rate will go up notably. Thus, the published (i.e., truthful) data tell only part of the story. Actual system accuracy in field operations may even be less than acceptable. This is the situation that created the need for a single measure of biometric system accuracy.

Equal Error Rate (EER)

The equal error rate is also called the cross over error rate and is the point, generally stated as a percentage, at which the false rejection rate and the false acceptance rate are equal. This has become ant important measure of biometric system accuracy.

The equal error rate provides a single measurement that is fair and impartial in comparing the performance of the various systems. In general, the sensitivity setting that produces the equal error will be close to the setting that will be optimal for field operation of the system. A biometric system that delivers a CER of 2% will be more accurate than a system with a EER of 5%.

Receiver's Operating Curve

Plotting a graph of FAR versus FRR gives a Receiver's Operating Characteristics (ROC) graph, which is shown in Figure 3.

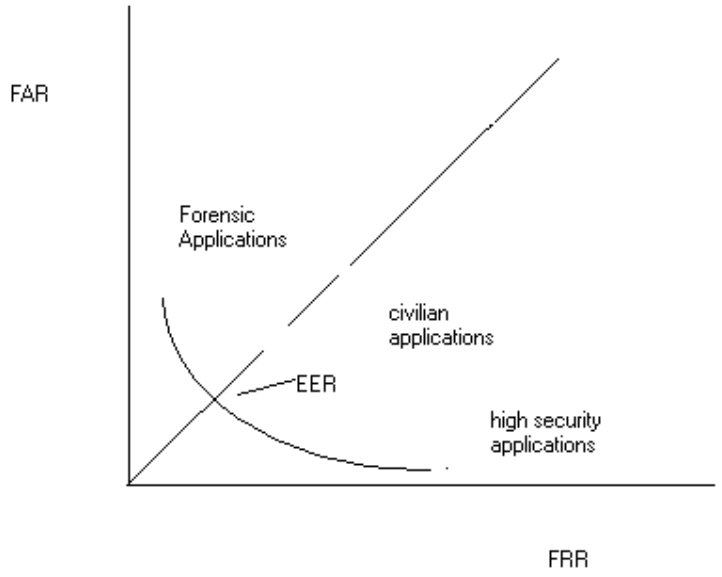

Figure 3: ROC graph : FAR versus FRR

The ROC is also called detection error trade-off curve by the National Institute of Standards and Technology (NIST) or more generally a performance curve. It is desirable that forensic application has a high FAR so it can try to maximize the chance of getting a suspect. In high security applications the False Acceptance Rate should be low.

In practice, sometimes the manufacturers will give lower false acceptance rates[9]. False matches are not exceptional for this technology. An known example\ is for instance Iridian Technologies, have claimed for their iris matching technology that no false match has been seen with their technology and that the changes of this happening are low. The test result of the International Biometric Group (IBG), USA, has learned a databases size upon which a false match was reported with only 130 persons. This give some doubts on the claims of Iridian of 1 in 1.2 million.

SPEED AND THROUGHPUT RATE

Speed is often related to the data processing capability of the system and is stated as how fast the accept or reject decision is returned. In actuality, it relates to the entire authentication procedure: stepping up to the system: inputting the card or PIN; input of the physical data by inserting a finger, aligning an eye, processing and matching of data files; returning of the accept or reject decision; and if a portal system, movement through and closing the door.

3. LIVE DETECTION AND TAMPERING CONTROL

Many reports and articles have been published on the vulnerability of biometric systems to spoofing attacks[10]. One of the first reports was published by the Japanese researcher Tsotumo Matsumoto, who presented a study at the International Telecommunications Union's workshop in Seoul, Korea, showing that fingerprint readers can be fooled around about 80 percent of the time by a fake fingerprint of gelatin.

A student from the Yokohama National University showed several ways to create a fake finger. The first method from a cooperative subject and the second method with latent fingerprints that were left by a person on various surfaces. The gelatin and silicon cast fingerprint systems that he examined had success rates ranging from 70-100 percent depending on the method.

An overview[11] given in the German CT of tampering with these systems shows how to enter biometric systems with photographs of faces, with copies of the fingerprints, or even using the latent fingerprint on a scanner, with a print for an iris system etc. In most cases the manufacturers will respond with the information that the system is a prototype and that not all security measures have been implemented yet. The manufacturers of biometric systems are becoming more aware of the problem with tampering, and solutions are provided how to avoid the possibilities to tamper with there systems[12].

To examine what kind of measures companies will take against fraudulent use, a patent examination an overview of available US patent information is given below. In *Italic* text, a comment is given on this patent concerning possibilities to abuse the method described in the patent.

The patents describe ways of detecting if persons are alive and if someone tampers with the systems. For each method one can find a way of circumventing it (especially if someone has enough time to experiment with an unattended biometric system). Several other patents and information sources describe the method of computing a template which is used for the comparison. Depending on the implementation someone can reverse engineer the template and try to compute a biometric feature where also access is given.

In US2002/0095608 a switch is described against tampering with the electronic device. It is isolated from its power source, it is not possible to circumvent the access control feature. *Tampering with electronic devices is possible, especially if the system is unattended, so it is worthwhile for manufacturers to implement this patent..*

In US2002/0122571 a method is described against fraudulent copying of the digital stored biometrics information. *It is often also possible to get biometric information from latent prints etc.*

In US2002/0138768 a portable system is described for examining the biometric evidence further with a heartbeat waveform and by measurements taken by the reflecting light of subdermal layers of the skin tissues. *In my opinion this patent will not prevent spoofing if a thin silicon cast is used on a fingerprint, where the silicon is conditions.*

In US 2002/0146154 a method is described by detecting tampering with the system if the biometric sample is exactly the same as the enrolment data. Normally there should be dynamic changes in the applicant's biometric samples. *This method is easily to spoof with, since for tampering a slight difference should be made in the biometric sample.*

In US6373967 (California Institute of Technology) a system is described in which fingerprints must be entered in a proper sequence to be recognized by the system, which is known to the user. *This method is somewhat more difficult, unless someone else can see the sequence that is used.*

In US5719950 (Minnesota Mining and Manufacture Company : 3M) a biometric authentication system is disclosed. In this system the stored biometric data is compared with one non-specific biometric parameter of a physiological characteristic. Claimed is that it is possible to determine that an individual is not incapacitated, dismembered or deceased. From the Internet http://www.ait.ca/html/solutions/biometrics.html it appears that 3M is active in Biometrics for integrated solutions. *If the non specific biometric parameter is known, it might be also possible to spoof with it.*

US5737439 (Smartouch) describes an anti-fraud biometric scanner that determines if an object exhibits the characteristics of a live human. It has a scanning means for obtaining the biometric sample from the object, a blood flow detection. It is also determined if someone is trying to simulate blood flow. From the Internet not many products have been found from this company. One page that appears to be from this company is www.smartouch.net appears to be static. *Also this method can be tampered with by thin gelatin or silicon casts depending on the method that is used.*

US5987153 (Quintet) involves detection of fraud with biometric data such as signatures. If the signature is exactly the same as the stored signature, this is rejected. This patent anticipates US 2002/0146154. A link to Quintet hand writing verification can be found at http://www.quintetusa.com / *This one is the same as the one before, just make a small modification of the signature.*

Several patents (e.g. US62598705 (Dew Engineering)) describe the use of encryption for improving the security of these systems.

4. FORENSIC IMPLICATIONS

Forensic information may be available from biometric systems. An example of a case may be a hacker who uses a biometric identification system for accessing his computer. One problem is however that with most biometric systems one can tamper, especially if they are unattended. If there are suspicions that someone tampers with the biometric system, one should look for silicon casts of body parts and examine log files of the biometric access device.

From forensic perspective even more information can be extracted from the biometric access devices. If the biometric data is stored in a database in a standardized way, it is possible to find statistical data, and have more information on the uniqueness of a biometric feature.

It is expected, that biometric systems (if properly implemented) will result in more reliable identification of persons. If the systems are implemented at banks, borders, entries of buildings etc. more information is available on the location of a specific person at a specific moment. Use of this information by law enforcement can conflict with privacy law. However, as with other systems, it is expected that in the future, depending on countries and state laws, more cases can be solved based on forensic evidence from biometric systems.

REFERENCES

[1] J. Woodward, *Visa waiver countries set tight deadline by USA*, Biometric Technology Today, May 2002, p.2.
[2] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki in IEEE Computer, *An Introduction to Evaluating Biometric Systems* February, pp. 56-63, 2000.
[3] http://www.frvt.org/default.htm
[4] http://www/bioapi.org
[5] http://www.itl.nist.gov/div895/isis/bc/bcwg/
[6] http://www.oasis-open.org/home/index.php
[7] http://www.manist.org.uk/FP5%20Roadmaps/_BVN.pdf

[8] S. Nanavati, M. Thieme, R. Nanavati, *Biometrics: Identity Verification in a Networked World*, John Wiley & Sons; 1st edition (March 15, 2002)
[9] T. Prout, *False match blow for iris scan vendor*, Biometric Technology Today, Nov/Dec 2002, p. 1-2.
[10] M. Lockie, *Spoofing claims sting industry*, Biometric Technology Today, June 2002, p.1-12
[11] L. Thalheim,, "Biometrie" , German CT, c't 11/2002, page 114 translation in English at http://www.heise.de/ct/english/02/11/114/
[12] http://www.iris-recognition.org/counterfeit.htm