

FINAL REPORT

**“BIOMETRIC TECHNIQUES: REVIEW AND EVALUATION OF BIOMETRIC TECHNIQUES
FOR IDENTIFICATION AND AUTHENTICATION, INCLUDING AN APPRAISAL OF THE
AREAS WHERE THEY ARE MOST APPLICABLE”.**

***by
Dr. Despina Polemi***

INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS
NATIONAL TECHNICAL UNIVERSITY OF ATHENS

APRIL 1997

The opinions and views expressed in this report do not represent the official opinions and policies of
the European Commission

TABLE OF CONTENTS

1.EXECUTIVE SUMMARY.....	3
1. INTRODUCTION.....	4
2. GENERIC APPROACH OF BIOMETRICS	6
2.1 PERFORMANCE MEASUREMENTS	8
2.2 TEMPLATES	9
2.3 THREATS	10
2.4 CRITERIA FOR EVALUATING BIOMETRIC TECHNOLOGIES	13
2.4.1 <i>Criteria for the Biometric Methods</i>	14
2.4.2 <i>Criteria for the biometric systems</i>	15
2.5 STANDARDIZATION-TESTING-PROJECTS	16
2.5.1 <i>Standardization Bodies</i>	16
2.5.2 <i>Testing-Projects</i>	18
3. BIOMETRIC TECHNIQUES, SYSTEMS, DEVICES	21
3.1 PHYSIOLOGICAL BIOMETRIC TECHNIQUES	21
3.1.1 <i>Fingerprint Verification</i>	21
3.1.2 <i>Iris Analysis</i>	22
3.1.3 <i>Facial Analysis</i>	23
3.1.4 <i>Hand Geometry-Vein Patterns</i>	24
3.2 BEHAVIORAL BIOMETRIC TECHNIQUES.....	26
3.2.1 <i>Speech Analysis</i>	26
3.2.2 <i>Handwritten Signature Verification</i>	27
3.2.3 <i>Keystroke Analysis</i>	28
3.3 NEW BIOMETRIC TECHNIQUES	29
3.3.1 <i>DNA Pattern</i>	29
3.3.2 <i>Sweat Pores Analysis</i>	29
3.3.3 <i>Ear Recognition</i>	29
3.3.4 <i>Odor Detection</i>	30
4. AREAS OF APPLICATIONS	30
4.1 PUBLIC SERVICES	30
4.2 LAW ENFORCEMENT	31
4.3 BANKING & FINANCE.....	32
4.4 PHYSICAL ACCESS CONTROL	32
4.5 COMPUTERS AND NETWORKS	33
5. CONCLUSIONS-RECOMMENDATIONS	33
ANNEX I: CRITERIA FOR BIOMETRIC TECHNOLOGIES	36
REFERENCES.....	38

1.EXECUTIVE SUMMARY

One of the most dangerous security threat is the impersonation, in which somebody claims to be somebody else. The security services that counter this threat are identification and authentication. Identification is the service where an identity is assigned to a specific individual, and authentication the service designed to verify a user's identity. The verifier can be identified and authenticated by what he knows (e.g. password), by what he owns (e.g. smart card) or by his human characteristics (biometrics).

The main objective of this study is to review and evaluate the biometric technologies including an appraisal of the application areas. It is difficult to make an objective and accurate evaluation on these technologies, since testing these systems involve special laboratories, test subjects and trained staff. This study is based on the available literature such as papers, technical reports, evaluative studies, manufacturers and designer claims.

In this study we examine the two categories of biometric techniques. The *physiological* based techniques, which measure the physiological characteristics of a person. These include: fingerprint verification, iris analysis, facial analysis, hand geometry-vein patterns, ear recognition, odor detection, DNA pattern analysis and sweat pores analysis. The *behavioral* based techniques, which measure the behavior of a person. These include: handwritten signature verification, keystroke analysis and speech analysis.

There are two basic concerns in these technologies: the error tolerance and the storage of the templates. The setting of the error tolerance of these systems is critical to their performance. Both errors (*False Rejection* and *False Acceptance*) should be low and they should both be quoted by the manufacturers.

The recorded biometric measurement of a user (*template*) can be stored in various places depending on the application and the security requirements of this application. The templates can be stored in the biometric device, in a central data base or in plastic cards. Trusted Third Party (TTP) services can provide security in transmitting and managing the templates when stored in a central database.

Reliability and acceptance of a security system depends on how the system is protected against threats and its effectiveness to identify system's abuses. There are various sources of threats that the biometric technologies face which they can fall into three main categories: physical, human and technical. We list and describe these threats in order to examine how each biometric technology addresses them.

Based on the literature, criteria are listed in this study, for evaluating the biometric methods and devices. The first set of criteria is formed to evaluate protocols, algorithms and codes implemented in the biometric systems. The second set will be used to evaluate operational, technical, financial and manufacturing aspects of these systems.

Lack of standards and independent testing are the weak points of these technologies. In this study the various standardization bodies seeking to develop standards are listed. The activities of other associations, that can be found helpful towards this effort, are also described. Various U.S. and European biometric projects have been described in order to provide knowledge and information for these technologies and their various applications.

Biometric technologies are applied in the following sectors: Pubic Services, Law Enforcement, Banking, Physical Access Control and Computer & Networks. It has been concluded that TTPs can provide confidence in these applications where the biometric templates are stored in a central data base.

1. INTRODUCTION

One of the most dangerous security threats is the impersonation, in which somebody claims to be somebody else. The security services that counter this threat are identification and authentication. Several definitions can be found for these services.

For example in [67], identification is defined to be the association of data with a particular principal, where a principal is an identity having one or more distinguishing identifiers associated with it (e.g. human users, physical/logical entities). In the same reference, authentication is defined to be the state by being true, real or genuine; worthy of acceptance by reason of conformity to fact and reality; of unquestioned origin; not copied, original; properly qualified; possessing authority not open to challenge.

In EU's glossary [19] authenticity is defined as follows " the avoidance of lack of completeness or accuracy in authorized modification to information".

The OSI authentication framework (ISO10181-2, sec. 5.1) implies by authenticity the service which provides assurance of the identity of a principal. Authentication services can be used by entities to verify purported identities of principals. A principal's identity which has been verified is called an authenticated identity.

In this study authentication is regarded as distinct from identification. In particular by identification we understand the process whereby an identity is assigned to a specific individual, e.g. a name; and by authentication the process designed to verify a user's identity.

The original need for identification was social, as transaction became more complex this need became economic. Names was the first means of identification, in particular surnames were used in Britain in 1066 [17], [35]. In 1538 in the reign of Henry VIII parish priests keep registers of births, deaths and marriages for identifying purposes. Passports were known to English law in 1300 [29].

There is a variety of means for identifying a person's identity:

- appearance (how the person looks, e.g. height, gender, weight)
- social behavior (how a person interacts with others)
- name (what the person is called)
- codes (what a person is called by an organization)
- knowledge (what the person knows)
- possession (what the person owns)
- bio-dynamics (what the person does)
- natural physiology (who the person is, e.g. facial characteristics)
- imposed physical characteristics (what the person is now, e.g. tags, collars, bracelets).

The goal of authentication is to protect a system against unauthorized use. This feature enables also the protection of subscribers by denying the possibility for intruders to impersonate authorized users. Authentication procedures are based on the following approaches [86]:

- *Proof by Knowledge.* The verifier known information regarding the claimed identity that can only be known or produced by a principal with that identity (e.g. passport, password, personal identification number (PIN), questionnaire).
- *Proof by Possession.* The claimant will be authorized by the possession of an object (e.g. magnetic card, smart card, optical card).
- *Proof by Property.* The claimant directly measures certain claimant properties using human characteristics (e.g. biometrics).

Members of industries, hospitals, banks, airports carry ID cards, punch passwords or PINs in order to identify themselves. In government and conventional environments, security is provided through badges, provision of information for visitors, issuing of keys [15]. These are the most common means of identification since they are the easiest to remember and the easiest to confirm. However these means are the most unreliable putting all components of security at risk.

IDs can be stolen, passwords can be forgotten or cracked. According to a UK poll one in three people write down their PIN number [64]. Security breaches resulting access to restricted areas of airports or power plants have caused terrorism. Although there are laws against false identification [30] incidents of intrusions and unauthorized modifications to information/systems/organizations occur daily with catastrophic effects. Credit card fraud is rapidly increasing causing bankruptcies [10], [21]. Children have been kidnapped from day care centers after being released to strangers. The "milk carton" approach for identifying children whose identity has been changed has not been very effective. Traditional technologies are not sufficient to reduce the impact of counterfeiting [65]. Additional convenient security barriers are needed as our society gets more and more computer dependent.

Biometrics, the use of biology that deals with data statistically, provides an answer to this need since the uniqueness of an individual arises from his personal or behavior characteristics with no passwords or numbers to remember. Biometric systems verify a person's identity by analyzing his physical features or behaviors (e.g. face, fingerprint, voice, signature, keystroke rhythms). The systems record data from the user and compares it each time the user is claimed.

Biometrics has been known for a long time. Alphonse Bertillon (France 1870) invented a system (Bertillon system) based on finger print analysis for identifying criminals. Francis Galton [37] trying to improve the Bertillon system proposed various biometric indices for facial profiles and he established an Anthropometric Laboratory. Since that time many facial measurements have been developed [42], [72].

The most common biometric techniques are:

- Signature Verification
- Retinal Analysis
- Facial Analysis
- Fingerprint verification
- Hand Geometry
- Voice Verification

Relatively new biometric methods are: DNA pattern, ear recognition, odor detection, sweat pores analysis, key stroke analysis, head analysis. We can categorize the biometric techniques into two classes:

- *Physiological based techniques* include facial analysis, fingerprint, hand geometry, retinal analysis, DNA and measure the physiological characteristics of a person.
- *Behavior based techniques* include signature, key stroke, voice, smell, sweat pores analysis and measure behavioral characteristics [82].

Biometric recognition systems based on the above methods can operate in two modes: identification mode, where the system identifies a person searching a large data base of enrolled for a match; and authentication mode where the system verifies a person's claimed identity from his previously enrolled pattern.

The reliability and acceptance of an information technology system depends on the effectiveness of the system and how the system is protected against unauthorized modification, knowledge or use. Systems based on physiological-based techniques are more accurate however the devices are larger and more expensive. Behavior based systems need further enhancements in identifying, verifying and adopting individual variability. They are cheaper to implement. It was found [25] that behavior based

systems were perceived as less acceptable than physiological based systems. Biometric techniques can be used to secure electronic transactions [49], government and commercial environments [15], [52], [3], [74], secure public and travel documents [60], information systems and networks.

The primary goal of this study is to review and evaluate the above biometric methods to address two major security concerns: identification and authentication. It is difficult to make an objective and accurate evaluation on the biometric technologies, since testing these systems involve special laboratories, test subjects and trained staff. Based on the available literature such as papers, technical reports, evaluative studies, manufacturers and designer claims we set criteria, define threats, evaluate biometric methods based on these criteria, list their present and future applications. These goals are achieved as follows:

A generic approach for all biometric methods is undertaken in the second chapter of this study. In this chapter technical aspects of the biometric systems are described in general. Biometric systems show variations in measuring human characteristics or behavior. A measure of variation is embedded into these systems which in technical language translates in tolerance of *Type I* and *Type II* errors (sec. 2.1).

The first step in implementing a biometric system is to collect and put on file a data set (template) representing the biometric measurement of a user. There are various places where we can store these templates (sec 2.2). In the next section (sec 2.3.) we describe the various threats based on the security objectives of identification and authentication. These threats arise from various sources (network and distributed systems, organizations, data base) since these sources are involved in the choice of a biometric system/device.

Based in the literature we describe various criteria that can be used in order to evaluate the biometric technologies (sec. 2.4). In Annex I, a complete list of criteria is presented. Setting security standards in any information system is important for its exploitation. Unfortunately standards have not been set for biometric technologies. However various attempts are taking place from various associations, testing centers and projects. In sec 2.5 we list and describe the various standardization bodies, testing and projects for promoting and setting standards for biometric technologies.

In the third chapter we treat each biometric method separately. Each section in this chapter considers one major biometric method, i.e. Fingerprint (sec. 3.1.1), Iris Analysis (sec. 3.1.2), Facial (3.1.3), Hand (sec. 3.1.4), Speech Analysis (sec. 3.2.1), Hand Written Signature Analysis (3.2.2) and other biometric methods (sec 3.3). In particular we describe these methods, we examine how the corresponding technologies respond to the criteria and threats listed in sec. 2.3, 2.4. We then list the application areas and products.

In chapter 4, an appraisal of the areas where biometric technologies are most important is presented. In particular applications are presented in the public services sector (sec. 4.1), law and order (sec. 4.2), banking (sec. 4.3), physical access control (sec. 4.4) and computers & network (sec. 4.5).

This report ends with chapter 5 where conclusions are drawn. A complete list of products, companies (obtained from the journal Biometric Technology Today) and manuals from certain vendors are provided in a separate appendix.

2. GENERIC APPROACH OF BIOMETRICS

Authentication procedures are based on the following approaches [86]:

- *Proof by Knowledge.* The verifier knows information regarding the claimed identity that can only be known or produced by a principal with that identity.
- *Proof by Possession.* The claimant will be authorized by the possession of an object.
- *Proof by Property.* The claimant directly measures certain claimant properties using human characteristics.

The most common approach of user authentication is the proof by knowledge because of its simplicity and easy of implementation. *Passwords* are traditionally used in military applications, protocols for accessing computer systems, telecommunications, and banking. There are many reasons why this approach is unsafe: Users usually choose predictable passwords, they are also sophisticated computer programs for searching passwords. Passwords might not be securely transmitted through the systems to the legal users. Especially in network environment where an eavesdropper can easily pick up the password, which is changed infrequently and flows over the network. If this happens the eavesdropper can gain access to all resources.

There are four type of passwords [23]:

- *group passwords* are known to all users in the system. This kind of passwords are dangerous for all systems.
- *unique passwords* for each individual are usually kept in a piece of paper instead of being memorized. This puts the security of the system at risk.
- *non-unique passwords* which are used to confirm a claimed identity. A short password is given to users where identification depends on a long number stored in a card (e.g. magnetic card). Unfortunately these numbers can be read and changed.
- *passwords which change each time* a system is accessed have the disadvantage that a list of password should be kept at the central system and a copy should be distributed to each user. The mishandling of these lists may lead to disclosure. The secure transmission of passwords from a central to legal users is a big problem.

Questionnaire is another method used in this approach. A list of questions is answered by individual users and their answers are used to distinctively identify them. However if someone knows the user well enough he can answer these questions and impersonate his identity. This threat makes the method very weak.

Passwords and questionnaires are providers of minimum security they are not capable to stop a malicious hacker. Therefore the other two approaches are more sophisticated alternatives to address the authentication concern. The proof by possession approach is considering the use of cards. The cards that can be used depending on the application are:

- Magnetic Stripe Cards
- Radio Frequency Identification Cards (RF-ID) and Tags
- Optical Memory Cards
- Smart Cards

1. *Magnetic Stripe Cards* are highly acceptable since they have been used for a long time in various applications (automatic teller machine, point-of-sale operations, credit validation, access control) and they conform to ISO (International Organization Standard) [40]. Terminals using the cards are standardized. Magnetic cards are widely used in automatic teller machines (ATM) for credit validation, for access control to secure sites etc. The user identity is stored on the magnetic stripe. The magnetic card is used in combination with a PIN (personal identification number). The danger of using these cards is that the PIN might be stolen, the cards can also be easily copied.

New technologies have enhanced the magnetic cards by incorporating additional anti-counterfeiting techniques [64]. New techniques known as Brocade or Biotin allow biometrics templates to be stored on a magnetic stripe card since they store them coded. The VEINCHECK project considers these new techniques (see sec. 2.5).

2. *RF-ID Cards* contain a tiny radio transmitter activated with the receipt of a signal with a specific frequency. If a biometric template is stored in such a card it could be send to the biometric device directly from the user's wallet without him knowing it.

3. *Optical Memory Cards* have information encoded in them that can not be changed. The advantage of these cards is their large memory capacity which enables to install encryption mechanisms in them.

4. *Smart Cards* are plastic cards with embedded computer chips (memory only chips, logic-memory chips, microprocessors). These cards have their own operating system, programs and data. They are highly acceptable in Europe.

More advanced technology is used by smart cards which rely on VLSI chips for information storage and processing. These cards are inexpensive and they are used as health professional cards, telephone cards, banking cards, etc. Assuming that the card itself is authenticated there is a weakness since the card still needs to identify the cardholder by some means. One of the most common techniques is the cardholder to carry out a PIN check inside the card. However this identification method is vulnerable to attack.

The most advantageous cards are the ones which are equipped with a microprocessor since they can store the biometric template and perform the verification process. In the CASCADE [16] project a smart card with a 32-bit microcomputer system was built which is suitable for voice, signature or fingerprint biometrics. Biometric methods used in the proof by property approach is the most advantageous means of authentication since it can not be stolen or transferred to other people. One disadvantage is that a biometric PIN can not be changed.

2.1 Performance Measurements

There is an important distinction between traditional means of authentication such as passwords, PINs and biometrics. A password (or a PIN) when typed by a user will be either correct or incorrect, so the user will be either accepted or rejected.

Biometric systems show variations in measuring human characteristics or behavior. A measure of variation is embedded into these systems which in technical language this translates in tolerance of *Type I* (False Rejection Error) and *Type II* (False Acceptance Error) error. The proportion of false rejections is known Type I error and the percentage of false acceptance as the Type II error. The setting of the error tolerance is critical to the performance of the system. False rejection causes frustration and false acceptance causes fraud. Type I and Type II errors can be translated in false acceptance and false rejection curves which are related to system's sensitivity threshold setting. Ideally these curves must be at zero at some threshold and setting the system at that point would yield a zero false rejection and false acceptance error.

Realistically these curves have a cross over point (*equal error rate*) which is the threshold at which false rejection and false acceptance errors are equally likely. The lower the equal error rate the more accurate any particular device is. A tight threshold setting will reduce the potential for false acceptance errors but it would increase the false rejection errors.

All systems should be able to reset threshold to increase or decrease the level of security as necessary. User's acceptance should also be considered for setting the threshold. Therefore the application will dictate the best setting. Standards are sought to ensure the same criteria used to obtain accurate error-rate measurements [28]. In applications with medium security level a 10% Type I error will be unacceptable, where Type II error of 5% is acceptable. UK banking community set performance figure requirement 1 in 100,000 for Type I error.

Since the tolerance level is adjustable, there is a trade off between the two-errors. Some biometric providers take advantage of it and they only quote the best of the two. Independent tests involving many verifications should be carried out in order to prove the accuracy of the errors recorded by the biometric suppliers.

2.2 Templates

By a template we mean the recorded biometric measurement of a user. A template is associated with an identifier (e.g. PIN, password) in order to be called up when it is requested. The templates can be stored in Memory of Device, Central Data Base, Tokens or Plastic Cards [64].

The storage of the users' templates depends on the type of application that the biometric device will be used and the size of templates.

Memory of Biometric Device

The templates can be stored in the memory of the biometric device. The memory capacity of the various biometric devices vary. Storing the templates in the memory of the device enhances security since the templates are not transmitted. It is also economic since no additional cost is required for issuing cards to the users. However this is not the best choice if the application requires many users (e.g. criminals in different states) or if the users need to be verified in different locations (e.g. different bank branches, airports, welfare offices).

Central Data Base

The templates can be stored in a central data base if the number of users required by the application is large or remote verification is needed. The security aspect of storing templates in a central data base should be carefully considered. The security of the templates can be compromised because of:

- the misuse and abuse of the data base administrators/internal intruders
- their insecure transmission to remote biometric devices.

Factors that can cause the security compromised [64] are:

- vulnerable telecommunication systems and networks
- abuse of privileges
- vulnerable communication protocols and compression algorithms

If the public network itself is not secure then the templates transmitted over the network can be seen by some intruder or by some network administrator/employee. An expensive solution to this problem is the use of dedicated lines .

Before transmitting templates over the Internet, Internet security should be enhanced. The use of World Wide Web and its tools such as Netscape and Mosaic add threats to the security of the templates.

A solution can be the establishment of a TTP (or a network of TTPs) ensuring the safe transmission and storage of the templates and providing the proper data base security. One option might be establishment of a TTP service in the central office of the network that will be responsible for the key management, and the safe transmission of the templates. Another option might be the establishment of a separate TTP dedicated to the safety of the templates which cooperates with the TTP of the network.

If the compression algorithms, involved in the transmission, are vulnerable to a cryptanalytic attack the templates can be revealed. If the communication protocols are weak then the security of the templates is at risk. Tested compression algorithms and protocols against any known (or unpublished) cryptanalytic attack should be used in order to prevent this major threat. Even if standard protocols and algorithms are used, they still need to be evaluated since as a standard ages it becomes increasingly vulnerable.

Plastic Cards or Tokens

This method of storage enables users to carry with them their templates in identification devices. This method is most appropriate when:

- number of enrolled is large to be stored in a central data base
- users need to be verified remotely
- templates need to be transmitted fast

- sensibility and safety of transmission is a priority

2.3 Threats

Threats can be seen as potential violations of security with expected or unexpected harmful results, and exist because of a vulnerability in a system. If an unauthorized user invades into a system he/she can destroy information, operating systems, programs. They can disclose information or they can cause disruptions or interruptions (damage systems, networks, organizations, institutions).

In biometric technologies where communication networks might be used for transferring templates, or when LAN can be used in identifying users in an organization, or where the storage and transmission of templates from a data base is essential or when the biometric devices are installed in insecure organizations then the systems might be abused by abusing its components (e.g. networks, computers, algorithms/protocols, data base, organizations). Thus threats arising in these areas (telecommunication systems, networks, computers and organizations), become the threats that the biometric technologies face as well. If and how biometric technologies face these threats is critical in evaluating their effectiveness.

There are the following sources of threats:

- *Physical*, which include natural disasters (fire, storm, water damage) and environmental conditions (dust, moisture, humidity).
- *Technical*, is the equipment of a system (or software) which might fail to carry out its function (failure), or it might carry them out in an appropriate way (malfunction).
- *Human*, which is the main source of communication breaches. It includes unauthorized users who wish to damage a biometric system, and authorized users who misuse the system either deliberately or accidentally. The human threats can be further categorized into internal and external: Internal human threats are disgruntled employees, hackers, former employees, system administrators, LAN and data base administrators. External human threats arise from commercial espionage, government-sanctioned espionage, vendors, manufacturers, kids looking for kicks, nosy reporters.
- *Theoretical*, which includes the vulnerability of the algorithms, protocols, and mathematical tools used in the methods that they are implemented in the systems.

The threats that can be identified are:

- Intrusion
- Denial of Service
- Disclosure of Information
- Corruption of Information
- Unauthorized use of resources
- Misuse of resources
- Unauthorized Information Flow

Intrusion occurs when an attacker gains access to the central data base where the templates are kept, to the device itself and is able to use it and modify it in the same way as a legitimate user. Policies need to be geared against social engineering attacks as well, where an attacker uses ploys such as posing as a senior administrator and demanding an immediate change (i.e. password, encryption mechanism, renewal of templates etc.) to allow very important and urgent work to continue. Some attacks in this category will exploit weaknesses in operating system security and will not require the attacker to knock at the door, the door opens itself for them. System administrators need to be trusty since their power enables them to abuse their privileges in several ways:

- They can change the data base for personal gain or for other motivations.
- They can give themselves privileges to access others that do not belong.
- They can allow dishonest people gain access and abuse the system.
- They can falsify transactions.
- They can control the back-up process so the back-up file will be corrupted.

In an organization environment the employees can cause a lot of damage. There are unintentional leaks which fall into three categories [78]:

- An employee discovers an unsought way into a system or device.
- Security is focused in one area leaving others insecure.
- An "eyeball leak": someone observes a printout or CRT screen of information he/she is not allowed to see.

Intrusion can also occur by cryptanalyzing algorithms, discovering leaks of protocols, encryption mechanisms and the cryptographic techniques used in implementing the protocols and algorithms into the systems. In our days where parallel computers, dedicated chips and optical methods (bio-chips) provide high computing power, even standard algorithms that thought to be secure can be cracked.

Denial of service can be achieved in multitude of ways, for example by corrupting routing tables, by damaging stored data, by locking user accounts, by unacceptable users physical and emotional condition. Malicious code can be thought as an indirect denial of service threat. Most users are now familiar with the threat posed by viruses, worms, Trojan horses and genetic algorithms. If non standard software is used (i.e. from universities, from magazine covers, from a friend or a neighbor) virus can be spread into the systems that can have catastrophic effects such as deleting a whole hard disc of data. However new forms of malicious code are appearing all the time.

There are several classes of system abuses:

- *Impersonating/Masquerading.* An authorized user gains access to a system or to a central data base where templates are kept by imposing as an authorized user.
- *Exploitation.* An unauthorized user seeks to exploit a hole in a piece of software or cryptographic weaknesses of the algorithms and techniques involved. Exploits succeed because badly written software is the norm, security is generally added as afterthought, too many programs run with excessive privilege violating the least privilege principle, and few programs use the operating systems underlying security features.
- *External penetration.* An intruder is trying to make unauthorized use of the system or device.
- *Active Wiretapping.* Connection of an unauthorized device to a communication link or a system for the purpose of obtaining access and modifying data. The methods of modifying data are:
 - ◇ *False messages:* the intruder generates false messages, records, templates or control signals.
 - ◇ *Protocol Control Information:* The control information in the message frames is modified in order to send them to a wrong destination or to a destination of his preference.
 - ◇ *Data Portion Modification:* Part of the message is modified for achieving the intruder's purposes.
- *Eavesdropping/Passive Wiretapping.* Monitoring or recording data while the data is being transmitted over a communication link.
- *Traffic Flow Analysis.* Examining the flow of messages across a network. The frequency, length, and addresses (source and destination of messages is analyzed).
- *Replay.* Playing back a recording of a previous legitimate message or record.
- *Deletion.* The unauthorized user discards messages, or records passing on communication link. The data base administration can delete a template and replace it with another.

- *Denial.* The user denies the fact of sending/receiving a message or record of its original content. This could be extended in denying obtaining some services from the network and therefore arising problems in billing and accounting of the network.
- *Jamming.* The intruder misuses the resources of the system by swapping a communication line with bogus or dummy traffic so that real messages or templates may not be transmitted. A device or system itself may also be jammed.
- *Social Engineering.* People generally like being helpful and attackers exploit this ruthlessly. Social Engineering is very hard to protect against as it is essentially hitting a "soft" target and requires "soft" means of addressing it such as staff education, clear policies and mechanisms for reporting problems.
- *Transitive Trust.* This type of abuse takes advantage of the trust models used by remote services.
- *Cryptanalysis* of weak algorithms, cryptographic techniques used to implement protocols. This abuse is the most sophisticated since knowledge of many fields in mathematics and computer science is required (e.g. statistics, linear algebra, cryptography, dynamical systems, theory of algorithms, complexity theory), the most expensive (parallel computers, dedicated chips, sophisticated programs are involved), and the most dangerous since the system can get abused without a trace.
- *Data Driven.* This type of abuse takes the form of viruses and Trojan Horses. For example an attacker can e-mail the victim a postscript file with hidden file operation in it. Or the abuser can insert viruses into the system or device using a diskette destroying or corrupting data across organization's computers and destroying any network to which the computers are connected.
- *Magic.* These are abuses that nobody has thought of yet. Such attacks if and when discovered will be full of surprises. An illustrative (and possible) example is Racing Authentication, where an attacker is able to sniff packets as a legitimate user logs in with SecurID or other similar authentication token. The attacker mirrors the user's keystrokes and takes a guess at last digit or SecurID code, thereby winning the "race" with the user login. If the attack is successful then the attacker is granted access, and the user probably just thinks he has made a typing error.
- *Combination abuses.* Malicious unauthorized users are likely to use a combination of the above methods when seeking to gain unauthorized access or to deny service.
- *Security Analysis Tools.* There are several systems that will probe a computer to test for known vulnerabilities (Farmer, Venema's SATAN, tool). These tools can be used by system administrators to perform security audits, however can also be used by attackers to probe for weaknesses.
- *Legal Abuses.* People using information systems are subject to the specific laws (e.g. in general practice there is the Access to Health Records Act, Data Protection Act, Copyright, Designs and Patent Act, Computer Misuse Act, Access to Health Records Act, Health and Safety at Work Act). These laws describe DOs and DON'Ts to follow for protecting all three dimensions of security (i.e. confidentiality, integrity, authenticity). These can also provide hints for the abusers.
- *Physical Abuses.* An unauthorized user can steal, hide or transport discs, tapes, printouts, fax messages lying around, back up files, biometric devices in order to collect enough information to attack the system.

- *Untrained users* can abuse the system unintentionally only because they are untrained and they are allowed to access the system. They can initiate processes which can corrupt or destroy data on the biometric device or on the central data base where templates are stored.
- *System Control*. Because of a lack or non-use of system controls for file, format, range and other validity checks records can be unsafe and input errors can be maximized.
- *Replay Attack*. Some biometric devices are not mathematically capable of differentiating between live data (finger or voice prints from a live user) and recorded data. This might be catastrophic.

2.4 Criteria for evaluating biometric technologies

The reliability and acceptance of a system depends on the effectiveness of the system, how the system is protected against unauthorized modification, knowledge or use, how the systems provide solutions to the threats (described in sec. 2.3) and its ability and effectiveness to identify system's abuses.

In order to evaluate the biometric technologies we first need to evaluate the biometric identification methods that these systems are based on. Although most of the studies and surveys concentrate on the evaluation of systems and products little has been said on the theoretical strength of the biometrics methods implemented in these products.

These methods use data compression algorithms, protocols and codes. The algorithms employed in biometrics are similar, what is different is the technologies used to implement them in each biometric. These algorithms can be classified in three categories:

- statistical modeling methods,
- dynamic programming,
- neural networks.

Coding detection and tracking of characteristics are the major components in biometric procedures. These mathematical tools need to be evaluated. Mathematical analysis and proofs of the algorithms need to be evaluated by experts on the particular fields. If algorithms implement "wrong" mathematics then the algorithms are wrong and the systems based on these algorithms are (or will be) vulnerable. If the algorithms used in the biometric methods have "leaks", or if efficient decoding algorithms can be found then the biometric methods themselves are vulnerable and thus the systems based on these methods become unsafe.

Different algorithms offer different degrees of security, it depends on how hard they are to break. If the cost required to break an algorithm is greater than the value of the data then we are probably safe. In our case where biometric methods are used in financial transactions where a lot of money is involved it makes it worth it for an intruder to spend the money for cryptanalysis.

The cryptographic algorithms or techniques used to implement the algorithms and protocols can be vulnerable to attacks. Attacks can also be conceived against the protocols themselves or aged standard algorithms. Some algorithms are only registered in the ISO and not checked for vulnerabilities. Thus criteria should be set for the proper evaluation of the biometric methods addressing these theoretical concerns.

The evaluation of the biometric systems is based on their implementation. There are four basic steps in the implementation of the biometric systems [13], [50] which impose the formation of evaluative criteria.

- Capture of the users attribute.
- Template generation of the users attribute.
- Comparison of the input with the stored template for the authorized user.
- Decision on access acceptance or rejection.

The reference used in formulating the desirable criteria for selecting a biometric method and system are: [17], [47], [66], [44], [23], [63], [5], [75], [76], [46], [28]. A complete list of these criteria follows. The undergoing ESPRIT project BIOTEST will also develop criteria and measures for evaluating biometric techniques, which unfortunately were not completed when this report was written.

2.4.1 Criteria for the Biometric Methods

The basic tools involved in any biometric method are: algorithms, codes, protocols, and a data base for storing templates. Therefore criteria should be set for evaluating these tools. In many environments (e.g. military and governmental) where security strength is most important a biometric system will not be adopted if the method that it is based on is not secure. .

1. Correct Algorithms

The mathematics implemented in the algorithms are correct.

2. Secure algorithms

Algorithms that are easy to break put any security architecture at risk however well built. The techniques used to implement the algorithms should be either unconditionally or computationally secure.

- *unconditionally secure*: no cryptanalytic techniques available for breaking the compression and other algorithms involved in the methods given infinite computing resources.
- *computationally secure*: If cryptanalytic algorithms can be found then the amount of data needed as input to a possible attack can not be stored in present and future computing systems. The time needed to compute the attack can not be performed with present or future computing resources (high time complexity). The amount of memory needed for the attack is not (will not be) available in present and future computers (high space complexity).

3. Good choice of keys The choice of keys is important.

4. Strong codes

- no efficient and robust decoding algorithms should be available.
- no efficient and robust decoding algorithms can be found.
- the decoding (if it exists) should be an NP-complete problem.

5. Secure Data Base

- data base administrator should be proven trustworthy it.
- template in data base should be securely stored, distributed and managed.

6. Safe protocols

- the cryptographic algorithms used in the protocols are secure.
- the cryptographic techniques used to implement the protocols are secure.
- no cryptographic attacks can be applied to the protocols themselves.
- analysis of Protocols.
- no flaws can be discovered in the protocols.

7. Secure Networks and Distributed Systems

If the templates will be transmitted over a network, the safety of the network should be evaluated.

The biometric methods need to be evaluated by specialists whose expertise is the evaluation of security systems. Some of these institutions are: NSA, RSA Laboratories, Swiss Federal Institute of Technology, Queensland University of Technology (Information Security Research Center), University of Belgrade (School of Electrical Engineering-EE-), University of Kentucky (Department of Computer Science-CC), University of Western Ontario, London, Canada (Department of Computer Science), Technion (Computer Science Dept.), HTL Brugg-Windisch, GRETAG Ltd, University of

Southern Louisiana (The Center for Advanced Computer Studies), University of London (Department of Computer Science), University of Louvain (Dept. of EE), University of Wincosin (Dept. of CC).

2.4.2 Criteria for the biometric systems

The reliability and acceptance of a biometric device depends on operational, technical, financial and manufacturing characteristics which set criteria for these devices. In Annex I, a complete and compact list of these criteria is presented.

Operational:

The devices should be *convenient* to use. For example the time required to perform its functions, such as enrollment, authentication, verification, should be minimum. In a supermarket queue or in a company's entrance (at rush hour, i.e. 9am, 5pm) where verification is to be performed, the time taken for verification is a major criterion for choosing a biometric device.

An important factor in the biometric technologies is *public acceptability*. In banking, security and public acceptability is a priority for choosing a biometric system since customers can choose another bank (e.g. eye pattern verification systems are not preferred). *User friendliness* is important for the device to be accepted by the public. A device is user friendly if it is easy to use, it is convenient, it satisfies the user's security needs, it conforms to contemporary social standards. It was found for instance that in Japan people do not like to place their palm where other people do [64]. The device should be *socially unpalatable*. Taking off the contact lenses in a public place and look into a scary looking device will not be accepted.

A device is public acceptable if it is *not discriminatory*. Human factors such as gender, age, profession, physical and psychological condition of a person should not influence the performance of the biometric device. People with soar throat or affected by dental anesthesia might face a difficulty in being verified by certain speech verification systems.

Other operational criteria are: *uniqueness* and *exclusivity*. The outcome of the authentication process should be unique, it should not change each time the user is verified by the biometric device so no other form of identification should be necessary or used. The device should be put in a safe place so it can not be collected by anyone on any occasion.

Technical:

All technical components of the biometric device contribute to its authentication time. For example if the templates are stored in the biometric device itself, the *space of its data base* should be sufficient. The *time* required to measure the human characteristics in order to create the templates and the *storing time* of the templates should be minimum. *The size of the device* should also be small. The setting of the *error tolerance* is important to the performance of these systems. Both errors should be explicitly quoted and they both need to be as low as possible. Some manufacturers quote only the best error, but this is misleading. The devices should be *simple* to use, *fast* and *precise*.

The devices should be able to perform well independently *of environmental conditions* (e.g. light, noise, heat, moist, smoke, dust). For example most hand readers can not be used in high or freezing temperatures, only in controlled indoor environments.

They should be *flexible* in adjusting threshold settings depending on the security level of the application.

Financial:

Cost is an important factor for choosing a biometric device. This might involve equipment cost,, installation and training cost. Most devices are expensive and this puts a barrier in the expansion of the biometric market.

Updating the templates can be a costly process. After the templates have been extracted by the users it is very hard to classify them. Devices that can operate only in controlled environments (e.g. where the temperature is constantly 15-25 C), it is costly to physically protect them. The *cost of the software* used by these devices should be also considered.

Administration support might also become a big expense.

Manufacturing:

The chosen biometric system should be supported by a number of manufacturers. National vendor support must be capable of accommodating national implementation.

Data must be exchangeable from one vendor's system to another at an acceptable level of defeat.

Different criteria will be considered in different applications. Not all criteria need to be considered in all applications. For example if the potential budget of a company is big, cost will not be considered as one of the criteria for choosing a biometric system. If a company wants to solve its security problem and it is also of limited budget then the choice will be based on putting cost and security strength as its primary considerations.

2.5 Standardization-Testing-Projects

Information technologies should be international in scope. Methods usable in Europe must continue to be usable in U.S.A. and vice versa. Therefore standardization is an important issue for choosing an information technology. Since biometric technologies are relatively new, standards are not issued as yet. However various committees, associations and organizations are formed in order to establish such standards. There is a big need for setting up standards for the biometric market to get exploited.

2.5.1 Standardization Bodies

Some of the organizations seeking the creations of standards for the biometric technologies are [23], [64], [8]:

- *The National Bureau of Standards* has published a useful guide (Guidelines on Evaluation of Techniques for Automated Personal Identification) which provide criteria for selecting an identity verification system.
- *European Union*. The European Union seeks clarification of various issues arising in biometrics requesting legislation considerations. These issues include: ownership of template, privacy, certification of safe verification products, security in data handling, certification/standards appropriate for each application. Definition of rights and responsibilities. The European Commission funds projects for the promotion of biometric technologies such projects are: CASCADE, BIOTEST.

The European Standard for access control -EN 50133-1 is under development requiring the system requirements for access control technologies to have a False Acceptance Rate 0.001% and False Rejection Rate less than 1%.

- *The Association for Biometrics* (AFB) founded in England in 1993 has developed a glossary of terms involved in biometric technologies which it has been accepted by the British Standards Institute. Its objective is the education of the public in the biometric technologies and products.
- *The Biometry Industry Standards Association* established in U.S.A has set out the goal to establish an independent testing site for the biometric technologies.
- *The Biometric Consortium* established in U.S.A in 1992 by the US Department of Defense aims to create standards which can be used to test biometric technologies for the benefit of all government agencies. NSA initiated the formation of the Consortium as part of its Information Systems Security mission. The goals of the consortium are [14]:
 - ◇ promote the science and performance of biometrics.
 - ◇ create standardized testing, establish evaluation center (National Biometric Evaluation Laboratory).

- ◇ information exchange between government, industry and academia
 - ◇ address the safety, performance, legal and ethical issues of biometric technologies.
 - ◇ advise agencies on the selection and application of biometric devices.
 - ◇ Their WWW address is : <<http://www.vitro.bloomington.in.us:8080/~BC/>>.
- *The Security Industry Association* in U.S.A has been formed to set up standards for the biometric technologies for the benefit of non government association.
 - *The ASR Workgroup* in U.S.A is an industry standard body which it developed to speech technologies with the objective the integration into systems. They developed Signal Computing System Architecture (SCSA) specification which is supported by the industry involved the integration of voice, data, and image technologies.
 - *U.S. Army's Facial Recognition Technology Program* aims to establish a basic performance standard for facial recognition algorithms, and to improve algorithm performance.
 - *International Civil Aviation Organization (ICAO)* examines biometric technologies for enhancing passport and visas to machine readable documents.
 - *Federal Bureau of Investigation (FBI)* has developed standards for the exchange of data [78]. An algorithm called Wavelet Scalar Quantization (WSQ) developed by FBI, NIST and Los Alamos National Laboratory became a standard for the compression of fingerprint images.
 - *Other organizations* are: Australian Biotechnology Association, US Securities and Exchange Commission, Swiss Association for Artificial Intelligence (SGAICO) and the International Association for Pattern Recognition (IAPR).

There are various organizations/groups for setting security standards [78], [73], [59], ([21], v.4, n.8). These bodies should also get involved in setting up objective criteria and standards for the biometric technologies since their knowledge and experiences will be very valuable.

These organizations are involved in the following activities:

- *International Electrotechnical Commission (IEK)* founded in 1906 is the first standardization body. Its objective is to promote international co-operation on all questions of standardization and related matters in the fields of electrical and electronic engineering. Its World Wide Web (WWW) address is: <<http://www.hike.te.chiba-u.ac.jp/ikedai/IEC/home.htm/>>.
- *The National Institute of Standards and Technology (NIST)* a division of the U.S. Department of Commerce created in 1987. Standards developed in NIST are used in private and in government. NIST issued DES, DSS, SHS and EES. Its WWW address is: <<http://www.nist.gov/srd/>>.
- *The Clinton Administration:* The President asks NIST to create standards. Encryption products when used outside the United States are controlled for preventing US's foreign policy, its national security interests and the safety of the citizens of the other countries. In November 15, 1996 The President William J. Clinton signed executive order transferring jurisdiction of encryption technology. This order liberates the export policies applied in commercial US encryption products [18] such as biometric technologies where encryption is highly used.
- *The Federal Telecommunications Standards Committee (FTSC)* works closely with NIST in assisting them in setting communications standards.

- *The International Standard Organization (ISO)* was founded in 1947 and it is located in Geneva. It is the biggest organization promoting the development of standards. Accredited representatives to ISO are:
 - ◊ The American National Standards Institute (ANSI)
 - ◊ The British Standards Institute (BSI)
 - ◊ Canadian Standards Institute (CSI) ISO has its own WWW page at: < <http://www.hike.te.chiba-u.ac.jp/ikeda/ISO/>>.
- *The National Security Agency (NSA)* created in 1952 by Harry Truman under the US department of Commerce. The Commercial COMSEC Endorsement Program (CCEP) is a 1984 NSA initiative to facilitate the development of computer and communications products, with embedded cryptography. The National Computer Security Center (NCSC) in NSA is responsible for the government's trusted computer program.

NCSC evaluates commercial security products (both hardware and software). It publishes the "Orange Book" whose actual title is: "Department of Defense Trusted Computer System Evaluation Criteria". The Orange book attempts to define security requirements, so that computer manufacturers can measure the security of their system objectively.

- *The Institute of Electrical And Electronics Engineers (IEEE)* This U.S. organization gets investigated by the U.S. office that gives recommendations on private-related issues (e.g. encryption policy, identity numbers, and privacy protections on the Internet).
- *The Internet Architecture Board (IAB)* is the manager of Internet, which is a network created by U.S. Department of Defense. IAB establishes protocols to be used in Internet such as Privacy Enhanced Mail (PEM) which is the application standard for encryption in the Internet.
- *Vendors-Professional-Civil Liberties Industry groups, and researchers* have distributed to set standards:
 - ◊ IBM developed DES in 1977 under an NSA contract which is confirmed as a standard by NIST until 1998.
 - ◊ RSA Data Security, Inc. a company formed by R. Rivest, A. Shamir, and L. Adelman developed the RSA public key encryption algorithm referenced in international standards.
 - ◊ Mykotronx, Inc is the only NSA approved chip maker for the Clipper and Capstone chipsets.
 - ◊ Electronic Privacy Information Center (EPIC) established in 1994 focus public attention on security issues to the National Information Infrastructure.
 - ◊ Electronic Frontier Foundation (EFF) has set out the goal to protect civil rights in cyberspace. Its main philosophy is that security is a social issue that everybody should have the right to know, and thus it is should be free of government restrictions.
 - ◊ Association for Computing Machinery (ACM) is an international computer industry organization founded in 1994 which deals with cryptographic policies and security issues.
 - ◊ Software Publishers Association (SPA) is a trade association of over 1000 personal computer software companies. Their main objective is the relaxation of export controls on cryptography.

2.5.2 Testing-Projects

Testing biometric devices is a costly process. It requires special laboratories, trained personnel, and specialized stuff. This is the reason why there are so few independent evaluative testing studies. The ones found during this study are listed below:

- *Miltre Evaluation Studies* [32], [23].
A significant study carried by the Miltre Corporation in 1977 on behalf of U.S. Air Force evaluated and compared several identity verification systems. These systems were: voice

verification, a system made by Texas Instrument Corporation, signature verification, a system made by Veripen Corporation and finger print verification a system made by Veripen Corporation. The Miltre evaluators concluded that the voice verification system was the most promising, however required further work to improve its performance.

- *Sandia National Laboratories* [46].
From December 1986 through April 1987 a number of tests on certain biometric products from various companies had occurred on behalf of the United States Department of Energy by Sandia Corporation. In that evaluation [58] the devices tested were:
 - ◇ voice verifier by T&T Technologies
 - ◇ eye retinal pattern verifier by Eyedentify Inc.
 - ◇ fingerprint verifier by Identix, Inc.
 - ◇ two hand profile verifier by Recognition Systems, Inc.
 - ◇ voice verifier by Voxton Systems Inc.

The results from this testing indicated a general improvement in verifier performance from a previous testing in 1985 [57]. Another set of testing started on 1989 whose outcome is described in [46]. The performance of six biometric devices of the following companies was tested:

- ◇ Recognition System Inc (Hand Geometry)
- ◇ Identix, Inc (Fingerprint)
- ◇ Capita Security Systems (Signature)
- ◇ EyeDentify, Inc (Retinal Scan)
- ◇ Alpha Microsystems, Inc (Voiceprint)
- ◇ International Electronics, Inc (Voiceprint)

It was concluded in this study that hand geometry was overall the user's favorite. the overall verification time was considered for :

- ◇ entering the PIN
- ◇ presenting the biometric feature
- ◇ verification or rejection

The Alpha-Microsystems Inc was the slowest followed by: the Capital Security System, Eye Dentify Inc, Identix Inc, International Electronic Inc and Recognition System.

- *San Jose State University testing.* In October 1995 the university started an 18-month testing of different biometric devices and their use in state and federal commercial driver license programs.
- *NIST* carries out tests of biometric systems (e.g. FACEit from National University of Singapore's Institute of Systems Science).

Biometric projects found that provide knowledge in the development and application of these technologies are:

- *PALMPRINT* project [6] was undertaken by University of Kentucky where a machine for automatic identification was developed using the geometric features of the hand. From their testing it was concluded that the machine satisfied the following requirements: ease of operation, short response, time and low false acceptance.
- *FAST* (Future Automated Screening for Travelers) project promoted by World Travel and Tourism Committee uses hand geometry and finger print verification to allow travelers to enter countries through automatic passport control barriers.
- The program Immigration and Naturalization Service Passenger Accelerated Service System *INSPASS* [87], [43] uses hand geometry system to verify travelers of passport control of various US

airports. INSPASS stations have been installed in N.Y. (J.F. Kennedy) and New Jersey (Newark) airports.

- *PORTPASS* [14], [87], [43], [64] is an Immigration and Naturalization service project similar to INSPASS except that people in vehicles at borders are being verified and it uses voice recognition systems.
- *TASS* [14], [87], [79], [83] is a project from the Spanish National Social Security Identification Card using fingerprint technology installed in a smart card in order to verify social benefits recipients.
- *Connecticut Digital Imaging Project* began in January 1996 sponsored by the State of Connecticut Department of Social Services for Welfare recipients.
- *Caller Verification in Banking and Telecommunications (CAVE) project* partially funded by the European Commission will be completed in June 1997. Its goal is to use speaker verification techniques in telephone banking, home shopping and information services.
- *CANPASS* [87], [43], [61] airport system project signed in February 1995 by US President Clinton and Canadian Prime Minister Jean Chretien and ended in November 1995 is a secured immigration system based on fingerprint and memory optical cards. The system is installed at Vancouver international airport. Its objective is to ease the passage of people and goods between US and Canada.
- *VEINCHECK project* started in November 1995 in EU framework IV programme. It involves UK technology transfer group coordinating the consortium which includes inventor Joseph Rice of Veincheck systems and two Dutch companies will evaluate Veincheck system and investigate the potential market for it which is based on analyzing the vessel structure in the back of the hands [69].
- *CASCADE* (Chip Architecture for Smart Cards) [16] is an ESPRIT project funded through OMI (Open Microsystems Initiative). Its main objective is to build a new generation of chips for portable electronic devices. Applications are: GSM phone systems, multi-service cards, electronic purse, personal digital assistants PCMCIA cards, health care, pay T.V. and video information services, multi-media information services, intelligent agent services, transport control systems, secure access systems, passport cards. CASCADE has produced a forecast of the potential market for smart cards holding biometric templates. The consortium consists of: GEMPLUS, ARM (Advanced Risc Machines), Domain Dynamics Limited, NCS, NOKIA, UCL, RD2P, DASSAULT AT, ARTTIC.
- *BIOTEST project* is an important 27-month ESPRIT project starting in 1996 which is very promising since its primary objective is to form independent testing methods so that manufacturers will be able to evaluate their products by the project's developed standards, measures, and criteria. Users will be able to compare the various biometric techniques and products for their specific applications. One of the most important objectives of this product is the establishment of independent testing centers. There are seven European partners involved in the project (CR2A-DI, National Physical Laboratory, Sagem, SEPT, SIAB, STI) and thirteen biometric manufacturers and users in various applications areas.
- *National Science Foundation* funds many biometric projects such as improving signature verification techniques developed by the US signature company Communication Intelligence Corp.).

3. BIOMETRIC TECHNIQUES, SYSTEMS, DEVICES

In this chapter we will describe each biometric method separately; we will examine each method for each effectiveness. In particular we will examine how the methods respond to some of the threats and criteria described in sections 2.3 and 2.4. Unfortunately we do not have an objective, accurate and complete evaluation on the biometric technologies, since testing these systems involve special laboratories, test subjects and trained staff. Based on the available literature such as papers, technical reports, studies, we will evaluate the techniques.

We will list the available and under development biometric systems and the corresponding companies. We gather this information from the journal Biometric Technology Today. (The management was kind enough to send me a complete list which I am submitting in Appendix. Manuals and brochures of certain products that manufacturers send me will be also submitted in that Appendix). For each method the areas of applications will be listed. This information was gathered from customer lists of manufacturers.

We hope that the future testing will consider the threats and criteria listed in sections 2.4 and 2.5.

3.1 Physiological Biometric Techniques

The biometric techniques described in this section measure the physiological characteristics of a person.

3.1.1 Fingerprint Verification

The patterns and geometry of fingerprints are different for each individual and they are unchanged with body grows. The classification of fingerprints are based on certain characteristics (arch, loop, whorl). The most distinctive characteristics are the minutiae, the forks, or endings found in the ridges [54] and the overall shape of the ridge flow. The fingerprint systems available for recognizing these characteristics are complex. Some systems are not capable of differentiating a fingerprint from a live user or a copied fingerprint. Finger surgery, injury, condition of hands might effect the performance of the systems. The method has also the problem of public acceptance.

Fingerprint systems can be used in law enforcement and in other applications. These two types of systems are different. In law enforcement applications fingerprints are compared (usually manually) with a large store of fingerprints where in other applications the fingerprint is stored once and it only checks that fingerprint. This technology is mostly used in welfare, immigration, law and order and banking applications. Federal Bureau of Investigation develops a nationwide digital data network in order to determine an identification and match it with prior records. This network will provide quick access to a new integrated Automated Fingerprint Identification System (AFIS) [14], [12] and will speed up suspect identification.

Such network will also be developed in US with children fingerprints in order to identify a child (whose identity might have been changed) by comparing the fingerprints against a national data base of children's fingerprints.

Effectiveness

Operational:

Fingerprint verification is associated with criminality and in many environments (e.g. medical) fingerprint technology would not be acceptable. In order to avoid the association with crime fingerprint should be stored in a card and not in a large central data base. It should be also emphasized that fingerprints can not be reproduced in no law enforcement applications. In banking it is acceptable if it is used for preventing card fraud. This was shown from a research conducted by UK's Plastic Fraud Prevention Forum. In this research the consumers opinion was asked on the following identification technologies: PIN, signature, fingerprint. The result was that fingerprint was the preferred as very secure, fast, reliable and easy to use.

Fingerprint systems can not be used by people with missing fingers. People with injured or swollen fingers might have a problem in being verified by these systems. In working environments where workers need to wear gloves (e.g. power plants, medical or chemistry laboratories) this method of identification will not be appropriate. Age, gender, occupation, race and environmental factors influence the validity of the fingerprint systems. A young female mineworker's fingerprint causes difficulties in the verification process [64].

Technical:

Fingerprints and palm prints are extremely accurate since they rely on unmodifiable physical attributes, but their use for access security requires special input devices. These devices are not always compatible with standard telecommunications and computing equipment. Thus they are undesirable for remote access by traveling users. Some finger recognition systems concentrate only on the location and identification of small areas of details whether or not such areas are identical. Neural approaches allow automation of the fingerprint encoding process which allows higher matching performance. This is particularly useful in searching a crime image to the files of prints of other convicts [54].

A fingerprint verifier can work with card systems such as smart cards and optical cards, to perform identity verification. It provides social welfare security by using cards such as an ID card, drivers licenses, passports, credit cards. The GAO report [39] says that "fingerprinting may be the most viable option" among the various biometric methods investigated which were: voice verification, hand geometry, signature verification, retina scanning. The CASCADE project claims that fingerprints is the best technology to reduce passenger's clearance time through customs.

Applications:

- Medical & Insurance Industry
- Government Agencies
- Identity Authentication
- High Power Reactor Stations
- Airport Traffic Security
- Identification of Missing Children
- Computer access or transaction control
- Physical Access Control
- Banking
- Information Security
- Police Department
- Immigration and Naturalization Services
- Welfare & Unemployment Benefit Recipients
- Database management systems
- Computer Database Security Control

Products:

- WinFing 3.1 (PrintScan International, U.S.A.)
- Fingerprint Scanner (The National Registry, U.S.A.)
- FingerCheck (Startek, Twaiwan)
- FingerScanner (FingerMAtrix, U.S.A.)
- FingerScan (Australia)
- TouchPrint 600 (Identix, U.S.A.)

3.1.2 Iris Analysis

Ophthalmologists originally proposed that the iris of the eye might be used as a kind of optical fingerprint for personal identification [22], [1], [34], [70], [24]. Their proposal was based on clinical results that every iris is unique and it remains unchanged in clinical photographs.

The iris consists of trabecular meshwork of connective tissue, collagenous stromal fibres, ciliary processes, contraction furrows, rings, colorations. All these constitute a distinctive fingerprint that can be seen at a distance from the person. The iris trabecular meshwork ensures that a statistical test of independence in two different eyes always pass. This test becomes a rapid visual recognition method [22].

The properties of the iris that enhance its suitability for use in automatic identification include [22]:

- protected from the external environment
- impossibility of surgically modifying without the risk of vision
- physiological response to light which provides a natural test.
- ease of registering its image at some distance from the subject without a physical contact.

In [22] it is mathematically proven that they are sufficient degrees of freedoms in the iris among individuals to impart to it the same singularity as a conventional fingerprint. Efficient algorithms are developed in [22] to extract a detailed iris description reliably from a live video image to generate a compact code for the iris and render a decision about individual identity with high statistical confidence.

Effectiveness

Public Acceptance: The iris recognition systems have public acceptability problems in many application areas. For example in the INFOSEC project Health Sign (1994) users in UK, Greece, Italy presented with specific technological choices for Electronic Signature Interfaces to Hospital Information Systems. The options included active badges, retinal scanners, fingerprint identification, speech analysis systems, and hand written signature. The outcome of the survey was that in UK retinal scanners were the least favorable where in Italy were unacceptable.

The iris recognition systems had public acceptability problems in the past because of the use of an infrared beam. The recent systems register the iris image easy at a distance from the user but users are still skeptical of this technology. Blind people or people with severe damaged eyes (diabetics) will not be able to use this biometric method.

Technical: The retinal blood vessels highly characterize an individual so accuracy is one of the advantages of this method of identification. Duplicate artificial eyes are useless since they do not respond to light. However medical research has shown recently that retinal patterns are not as stable as it was thought. They show critical variations when there is an organ dysfunction or disease [56].

Applications:

- Correction facilities
- Department of Motor Vehicle

Products:

- IrisScan 2020, System 2000 EAC (IrisScan, U.S.A.)
- IrisIdent System (Sensor, U.S.A.)
- 2001 (Eye Identify, U.S.A.)

3.1.3 Facial Analysis

The premise of this approach is that face characteristics (e.g. size of nose, shape of eyes, chin, eyebrows, mouth) are unique revealing individuals identity. This now increasingly developed method is expensive since it is using neural network methodologies. They use cameras to extract unique facial feature data which is stored on a chip card or a magnetic stripe card. The person swipes his card to a small camera to take an image. The software application on site compares the data with the person's stored data.

Effectiveness

Operational:

In the existing facial recognition systems certain restrictions are imposed by the user e.g. he/she should be looking straight in the camera with certain light in order for the system to analyze and

identify the person. However various new graph matching techniques will enhance the quality of picture decreasing the constraints [53].

The system will not be able to analyze people with imposed physical characteristics such as beard, hair style or with certain facial expressions.

Users find it very naturally to be identified by their face since this is the most traditional way of identification. It is highly acceptable.

Technical

Facial recognition systems are unable to cope with angles or facial expressions which are a little different from those used during the encoding process. The templates should be updated since changes occur in the facial skeleton during the human aging process.

Applications:

- Banking
- Airport Security
- Welfare Agencies
- Computer Facilities
- Telephone Companies
- Hospitals/ Health Care Institutions
- Police Authorities
- Credit Card Companies
- Security of Internet
- Buildings Security
- Drivers Licenses
- Voter Registration Processes
- Social Security Systems
- Vehicle Safety

Products

- Facial Data Base Systems (Dectel Security Systems, U.K.)
- True Face, True Face Cyber Watch (Miros, U.S.A.)
- Thermace, VIAS (Forensic Security Services, U.K.)
- FR1000 (Technology Recognition Systems)
- Sherlock Face Recognition (Facial Reco Associates)
- Facial Search System (Identicator, U.S.A.)
- KEN (Lawrence Livermore National Laboratory, U.S.A.)
- MufMaster (NeuroMetric Vision Systems)
- ZN-Face (Zentrum fur Neuroinformatik, Germany)
- FACEit (National University of Singapore)
- ARGUS (George Mason University)
- Face Pass (MIT Artificial Intelligence Laboratory)
- FACE-SOM (UMIST)
- Facial Recognition Software (University of Essex)
- Dextel Crime Net (Dextel Security Systems, UK)
- One on One Facial Recognition Systems (Identification Technologies International Inc., U.S.A)

3.1.4 Hand Geometry-Vein Patterns

This biometric method is based on the distinct characteristics of the hands, these include external contour, internal lines, geometry of hand, length and size of fingers , palm and fingerprints, blood vessel pattern in the back of the hand. They work by comparing the image of the hand with the previously enrolled sample. The user enters his identification number on a keypad and place his hand on a platter. A camera captures the image of the hand and then a software analyzes it. Other systems use cards where the user's hand is recorded [4]. This technology is mostly used in physical access control, law and order areas.

Effectiveness:

Technical:

Hand geometry systems are reasonably fast. They require little data storage space and the smallest template. They have short verification time. A technical problem that needs enhancement is caused by the rotation of the hand where it is placed on the plate.

The performance of these systems might be influenced if people wear big rings, have swollen fingers or no fingers. Dirt may also obscure the performance the details of the hand. The reconstruction of the bone structure of an authorized user's hand may be a reason for circumvention. In those systems that are based on three dimensional hand geometry where the three dimensions length, width, thickness are measured, although they are more secure there is still a chance of defeat. An artifact which is an accurate representation in all three dimensions may defeat the system [77].

Most of the hand readers are designed to be used indoors in controlled template environment since below freezing temperatures and temperatures over 110 F cause problems. The direction of the sunlight towards the platen might influence the hand picture. Various systems have been developed for obtaining vein patterns in the back of the hand which use various vein pattern matching strategies [20]. These systems are based on digitizing the vein patterns and applying statistical process control techniques [69] (see VEINCHECK project in sec. 2.5).

Operational

Sandia testing [46] conclude that hand geometry system was overall the user's favorite compared with fingerprint, signature, voice print, retinal. Although hand analysis is most acceptable in most countries, it was found that in Japan people do not like to place their palm where other people do [64]. Sophisticated bone structure models of the authorized users may deceive the hand systems. Paralyzed people or people with Parkinson's disease will not be able to use this biometric method.

Areas of Applications

- Airport Traffic
- Immigration and Naturalization Services
- Time and Attendance
- Hospitals/Medical Security
- Stock rooms/Equipment Storage
- Power Stations
- Casinos (access to money rooms)
- Universities/Research Laboratories
- Banking
- Employee Verification
- Super Markets
- Drug Stores
- Computer Room Access
- Welfare
- Prison Visitor/Inmate Control

INSPASS project claims that hand geometry is the most suitable technology for verifying travelers at passport control. Testing in various US airports occurred under this project that justified these claims.

Roger Kiel from the German Ministry of Interior claims that hand geometry is the preferred biometric technology for airport traffic. ([8], vol.4, n. 5, Sep.1996) because of its track record under the INSPASS project (see sec. 2.5).

Products

- Hand Geometry Readers (Computer Data Systems, U.S.A)
- Hand Geometry Readers, ID3D HandKey, HandPunch (Recognition Systems, U.S.A.)
- Digi-2 (BioMet Partners, U.S.A.)
- BioDentity System (Biometric Security Systems, U.K.)
- FastPass II (Biometrics, Inc, U.S.A.)
- Veincheck Systems (British Technology Group, U.K.)
- PG-2001 (Talos Technology Inc, U.S.A.)

3.2 Behavioral Biometric Techniques

The biometric techniques in this section measure the behavioral characteristics of an individual.

3.2.1 Speech Analysis

There are various characteristics of the sounds, phonetics, and vocals that an individual can be identified by. Vocal characteristics such as mouth, nasal cavities, vocal tract make the production of speech different for each individual. Although humans can use these characteristics naturally for identifying someone, it is hard for a computer system to analyze the voice characteristics.

The person speaks over the telephone or into a microphone attached system, then the system analyses the voice characteristics of that sample. Usually Fourier based methods is applied to extract a set of biometric features associated with the voice. These are coded into a data set or template. Finally the system compares it to the voice characteristics of a prerecorded sample. Furthermore the systems developed for doing so (e.g. AUROS speaker recognition system) can not respond on the danger that an individual's voice might change due to each physical and emotional state. This method also has the acceptability problem. It is mostly used in computer and telephone systems access control, in door entrance and vehicles security systems.

Once the European Union telecom market is liberalized in 1998, the telecom ministers will provide legislation covering voice telephone services. The market for voice-telephone biometric systems will expand.

Effectiveness

Theoretical

Some systems are based on a new technology called TESPAS (Time Encoded Signal Processing and Recognition) which is a simplified digital language for coding speech. It provides a simple way of generating a computer "signature" that defines any sound. It works by analyzing "snapshots" of a sound wave against time without calculating frequencies (something different than the classical Fourier analysis). This technology is spectacular and is applied in many different areas such as diamond drilling, security systems and voice identification. However the mathematical proof remains controversial [68]. In speech verification systems a very high complexity of computation is required.

Some systems are not (or will not be) mathematically capable of differentiating between real and prerecorded voices as digital recording systems get enhanced.

Technical

Speech verification is not as accurate as biometric verification based on physical characteristics such as fingerprint, palmprint, retina scans. However it is public acceptable since speech is the most natural form of identification [64]. It is a suitable technology for environments where "hands free" is a requirement. Systems developers combine speaker verification with other forms of security.

Computers find it hard to filter out background noise. Duplication of voice using a tape recorder is a major threat to these systems. Another danger is in anti theft biometric systems. In these systems physical damage (or removal) can occur to the devices if they are located.

Operational

Illness, fatigue, and stress are some of the factors that cause problems in the speaker verification systems available. The individuals' voice are changed over the years which make them hard to be verified [33]. Thus updating of the templates have to occur. This is costly since after the templates have been extracted by the users it is very hard to classify them. The techniques used (which are very complex) suffer from a number of limitations [62].

However it is less vulnerable to unauthorized access than key cards that can be lost and passwords and PINS that can be stolen [55]. Speaker verification can make a security system less vulnerable to

violation and more easily accessible from remote sites. Some systems have tedious enrollment procedures.

Women have more complex voice frequencies which makes them harder to be identified. People with soar throat or unable to speak will not be able to use such systems. People affected by alcohol, by dental anesthesia, by oral obstruction might face a difficulty in being verified by speech verification systems.

Although most developed systems have a certain tolerance range or even further they have a signal tone transmitter (Dialer) but more effective alternatives must be developed. A limited number of people can use it. Most systems recognize up to five different speakers by the word and the voice. As digital recording equipment become more and more sophisticated, the fear of reproducing someone's voice exists.

Some systems have problems with noisy backgrounds, however the use of TES (Time Encoded Speech) combined with artificial neural network architectures appears to be helpful in high noise environments [40], [81]. TES is a form of waveform coding first proposed by King and Gosling [51].

Applications:

- Anti theft systems for vehicles and doors
- PC and computer network access control
- Door entrance systems
- Hospitals (access to nursery)
- Benefit Payments
- Equipment to authorize chip and magnetic key cards
- Universities (access to laboratories, computer centers, student unions)
- Enforcement of bail, non custodial activities
- Telephone Networks
- Passport control
- Prison Payphones
- Pharmacy
- Aerospace company
- Fraud Control in prisons and correction facilities
- Air Force in air communications (identify pilots)

It has been announced that a portable speech recognition system for people with cerebral palsy will be developed [71].

Products:

- VOCAL, VOCAL SCW1, VOCAL ZKE (ABS, Germany)
- PIN-LOCK, voice verification system (T-NETIX, U.S.A.)
- Caller Verification System (Bell Security, U.K.)
- Tele-Matic (Speakez, U.S.A.)
- TESPAN/FANN (Domain Dynamic Limite, UK).

3.2.2 Handwritten Signature Verification

This biometric method is based on the fact that signing is a reflex action, not influenced by deliberate muscular control, with certain characteristics (rhythms, successively touches the writing surface, number of contracts, velocity, acceleration).

The systems developed based on this biometric method fall into two categories:

- Pen based systems are using special pens to capture the information.
- Tablet based systems use special surfaces to collect the data.

In the first class the pen is the measuring device which captures the information where in the second class, the tablet contains the measuring device. Some of the above systems use statistics in verifying a signature and some use event sequential methods. The items used in a statistical analysis include:

- total time of writing a signature
- measurements of spacing number of horizontal turning points
- number of times
- duration the pen touches the tablet.

In the event sequential methods the system divides the signature into independent events, and examines each piece separately. A number of signatures (depending on the system) are required for the enrollment process. At the time of verification the user is asked to sign. The system compares various aspects of its signature on a hierarchical manner. If a good match is not found between the signatures characteristics (shape, sequence of events, local characteristics) and the template then the template is rejected. The use of artificial neural networks make these systems more accurate and cheaper [41].

Effectiveness

Operational

Since signature is a familiar way in identifying individuals, hand written signature verification systems are highly acceptable. In a survey performed by a branch of a UK Post Office a signature verification system was preferred over the fingerprint system. People with Parkinson's disease will not be able to use such system. In countries where the illiteracy rate is very high this technology can not be used.

Some systems have difficulties with people that change their signature very radically. The Securisign system [26] can prevent access of people under the influence of drugs or alcohol. Other systems can not distinguish the pen from the palm pressure.

Financial

High cost of acquisition and processing hardware is required in these systems.

Applications:

- | | |
|-----------------|----------------------------|
| • Banking | • Internal Revenue Service |
| • Post Office | • Social Medicare |
| • Home Shopping | • Welfare |

Products:

- Signature Analyzer (PenOp Inc., U.S.A.)
- Rolls Royce Signature Verification (British Technology Group, U.K.)
- Electronic Signature Verification System (Quintet, U.S.A.)
- Cyber-SIGN (Gadix, U.S.A.)
- Signature Verification Software (Communication Intelligence Corp., U.S.A..)
- Countermatch (AEA Technology, U.K.)
- ID-007 (cadix International, Japan)
- IBM Transaction Security System (IBM. U.S.A.)
- Sign/On (Checkmate Electronice, U.S.A.)

3.2.3 Keystroke Analysis

This method which is under development is based on the typing characteristics of the individuals such as keystroke duration, inter-keystroke times, typing error frequency, force keystrokes etc.

Two kinds of systems are getting developed based upon static and dynamic verification techniques The static verifier uses a neural network approach while the dynamic verifier is using statistics. The static approach is where the system analyzes the way a username or password was typed using neural network for pattern recognition [9], [49], [36]. Dynamic approach is where the system verifies the person continuously with any arbitrary text input [36].

This is a method that can be offered as supplement to some secure authentication mechanism and not to be used independently. The performance of the method is affected by various circumstances of the human users, such as a hand injury or fatigue of the legitimate user. The systems developed for this biometric method are costly since they use neurological methods and dedicated terminals. Products under development for keystroke dynamics will come from BioPassword Security Systems, UK, Electronic Signature Lock Marketing, U.S.A., M&T Technologies U.S.A.

3.3 New Biometric Techniques

In this section we will describe more recent biometric techniques which most of them are under development.

3.3.1 DNA Pattern

This method takes advantage of the different biological pattern of the DNA molecule between individuals. Unique differences in the banding pattern of the DNA fragments occur. DNA prints were first used in 1983 in United Kingdom [84].

The molecular structure of DNA can be imagined as a zipper with each tooth represented by one of the letters: A (Adeline), C (Cytosine), G (Guanine), T (Thymine) and with opposite teeth forming one of two pairs, either A-T or G-C. The information in DNA is determined by the sequence of letters along the zipper [7]. Unlike fingerprint that occurs only on the fingertips, DNA print is the same for every cell or tissues of the body.

This method is widely used in identifying criminals. The basic concerns against this methods is the ethical and practical acceptability from the user. Time consumption for verifying an individual is also a big concern since DNA testing is neither real time nor unintrusive. DNA pattern recognition is a laboratory procedure that follows the next steps [7]:

- Isolation of DNA
- Cutting, sizing and sorting
- Transfer of DNA to nylon
- Probing

It is an expensive method and involves the provision of tissue or specimens which many people find demeaning. The area of application is criminal justice.

3.3.2 Sweat Pores Analysis

The distribution of the pores in the area of the finger is distinct for each individual. Based on this observation sweat pores analyzers have been developed which analyze the sweat pores on the tip of the finger. When the finger is placed on the sensor, the software records the pores as stars and stores their position relative to the area of the finger.

A system under development is: PCMCIA (Personal Biometric Encoders, U.K.)

3.3.3 Ear Recognition

The shape, size of the ears are unique characteristics of an individual. This technique is used in police in order to identify criminals.

Product: Optophone Ear Shape Verifier (ART Techniques, U.S.A.)

3.3.4 Odor Detection

The premise of this technique is that chemicals called volatiles makes the distinctive person's smell. A number of sensors are checking the different compounds that makes someone's smell. This method is under development. A system that is suppose to be completed in 1997 is Scentinel (Mastiff Electronics, U.K).

It is concluded that no particular biometric technique is utilized in an application e.g. access control is using hand analysis and speech analysis. No single biometric has dominated the market, the market is open and especially in Eastern European, Ex-Soviet Union countries and any other country where no identification technologies are used.

4. AREAS OF APPLICATIONS

In this chapter we will describe various present and future applications in the areas where biometric technologies are most applicable. These areas are: Law and order, Banking, Computers & Networks, Public Services and Access Control. It is hard to make an objective market survey since secrecy surrounds many of the application areas. The information in this chapter was mostly gathered from vendor's consumers lists, from the journal of Biometric Technology Today [8], from Emma's Newton report [63], from the projects listed in sec.2.5, and from the WWW page of Biometric Consortium (sec.2.5). Some ideas from the author are also included.

4.1 Public Services

A: Immigration Applications:

It is shown ([8] v.7, n.7) that in immigration applications, fingerprint is mostly used in North America, Africa, Middle East, Eastern Europe, Asia and Pacific where in Europe is used fingerprint analysis for criminal applications, i.e., Automated Fingerprint Identification System. It is also shown that fingerprint holds the largest share in the global market. Immigration applications include:

- *Passport Control:* Verify passengers through automatic passport control INSPASS (see se. 2.5) provide guidelines for this application.
- *Ease and secure the passage* of people and good between countries where visas are not required: CANPASS (see sec. 2.5) the pilot project involving U.S.A. and Canada is the most important project in this area. Such project is very important in Europe. With the Schengen Agreement where EU citizens are not required to show their passports CANPASS can provide guidance in European airports. It would enhance the economic union and the tourism. In Greece for example where tourism is the main source of income would be very valuable. Athens airport is a small and passenger traffic become a real problem in the summer time. Having a fast procedure to clear customs would solve the problem.
- not allowing *illegal aliens* to enter the countries holding false visas, and copied documents; monitoring illegal aliens in asylums.

B: Welfare:

In this area North America uses the fingerprint systems AFIS, Africa, Middle East, Asia and Pacific uses fingerprint and Europe uses equally fingerprint and signature. AFIS holds the largest share in the global market. ([8], v.7, n.7). Applications in this area are:

- *Benefit Payments:*
Social security benefits: Biometric technologies are used in verifying the legal recipients of social security, unemployment, and pension benefits. An important project in this area is TASS (see sec. 2.5). A future application can be the use of biometrics for home deliverable benefits. In Greece for example social security and pension checks are home delivered by the post man who has the responsibility of distributing the check to the legal recipients. They have been incidents where the

post man has given the checks to wrong persons. A portable biometric device carried by the post man will solve the problem.

- *Food stamps*: In U.S.A. food stamps are given to people with poor finances. They need to prove that they fulfill the requirements to receive these benefits. Many people sell or exchange their food stamps. The use of biometrics would help to verify the legal recipients and holders of food stamps.

Other applications are:

- medical insurance fraud reduction
- verifying recipients of aid to families with dependent children
- reconstruct voice of patients with cerebral palsy.

4.2 Law Enforcement

Biometric technologies in this area of applications are: finger, hand, iris, signature and voice. It has been found ([8], vol.7, n.7) that in this sector of application fingerprint technology is mostly used in Middle East, Asia and Pacific. Africa equally uses AFIS and fingerprint. Hand geometry is mostly used in North America and Europe, where hand and signature are equally used in South America. Hand geometry holds the biggest share in the global market in the law and order sector. Applications in this area are:

- *Prisoners, Prison Visitors, Inmate Control*: ensure that the persons leave the prisons are privileged visitors and staff and not the prisoners. FBI's Integrated Automated Fingerprint [14] will replace the manual fingerprint system in order to reduce response time.
- *Patrol cars* will have the capability to capture fingerprints and relay the information to local state by the fall of 1999 [85], [14].
- *The bureau of printing* and engraving will use biometrics to prevent any loss of currency [14]. The department of defense is considering biometrics for enhancing computer network security. The Federal Aviation Administration is researching biometrics for airport security applications.
- *Home confinement*: This is a common penalty in the U.S.A. where instead a person to be in prison he is prisoner in his own house and he has to stay in his house for certain hours per day. Voice verification systems are the biometrics used in order to verify the person by his voice when automatically is telephoned in his house.
- *Voting*: Ensuring that the person has not voted twice, that he is a citizen of that country in the right age. The Colombian Legislature uses hand geometry to secure the voting process.
- *Identification of Criminals*. AFIS technology is used in identifying criminals along the states of U.S. creating a central data base of criminals' fingerprints.
It would be useful to apply this idea in Europe. In particular, similar national data bases with fingerprints can be formed managed by national TTPs. Then a network of these TTPs can be formed guarding Europe.
- *Identification of Missing Children*: When children's identity has been changed a biometric verifier can identify the child by comparing the fingerprints against a national data base of children's fingerprints. Fingerprint technology will be used in U.S.A. for this purpose ([8], Nov. 1996, p.3). Using biometric technologies for this purpose will be helpful in Europe as well. TTPs could provide security if used as in the previous application.
- *Safe guns*: Most murdered police officers in U.S.A. are murdered by their own gun. Children all over the world get killed by their parents' gun. NIS has started a program whose objective is to built a "safe gun" which it can fire only after verifying that the person holding it is allowed to hold it.

- *Drug Trafficking*: The Californian Department of Justice protects the sensitive data base with drug trafficking related information using fingerprint technology.

4.3 Banking & Finance

It is shown that in banking fingerprint is used mostly in North America, Africa, Middle East, Europe, Asia and Pacific, where hand analysis is used in Eastern Europe. Fingerprint is the biometric that holds the largest share in the global market in this area ([8], v.7, n.7). Applications include:

- *Automated Teller Machines (ATM)* Securing the "front" of ATMs e.g. payment wages, transactions made in ATMs. Securing the "back" from fraud made by people with inside information.
- *Home Banking*: Secure transactions/payments made through telephone using voice verification technologies.
- *Credit Card*: ensuring the security of credit cards from stealing them. Fingerprint was the preferred choice.
- *Point of Sale*: transactions made in the branches
- *Safety Boxes*: Secure the bank's safety boxes.
- *access control*: Verification of bank personnel, customers and
- *Wage assurance*: Ensuring that the monthly salary and wages are cashed by the legal recipients.
- *Securing Transactions*: Ensuring that legal transactions were made by the bank to the legal customers.
- *Customer's data*: Ensuring that the correct data were given by the different branches when they were automatically called.

4.4 Physical Access Control

In this area of applications is shown ([8], vol.7, n.7) that in America and Eastern Europe hand geometry is mostly used where in Europe, Asia and Pacific the most common biometric is fingerprint. It is also shown that hand geometry holds the biggest share in this application area. Specific applications are:

- *Building safety*
- *Secure access to buildings*
- *Aircraft safety*
- *Plant, engine and gear box condition monitoring*
- *Casinos*
- *Hospitals: securing medical records, patient records*
- *Universities (laboratories, computer rooms, dormitories, student unions)*
- *Power plans (restriction to access sensitive equipment)*
- *Day care centers/kindergartens: verifying the people picking the children)*
- *Defense forces/government agencies*
- *Protecting electoral and voting procedures*
- *Olympic games*
- *Recreation and Amusement Parks: verifying the legitimate users of weekly passes.*
- *Time and attendance of employees*
- *Entry and exit to psychiatric ward*

- *Pharmacy*
- *Airports* (access to restricted areas of the airport)
- *Vaults and Safes*
- *Access control in health clubs/ casinos/ chemical, telephone companies/ organizations/supply stores.*

4.5 Computers and Networks

In this area of application voice analysis is mostly used in Europe, fingerprint analysis is used in Asia and Pacific where signature and voice are equally used in North America. Voice holds the biggest share in the global market ([8], vol.7, n.7). Applications in this area include:

- *Computer Terminals* (they can get protected for securing sensitive data e.g. governmental documents, medical data)
- *Telephone Companies* (enhance calling cards, access to company telephone system)
- *Communication network and mobile phones*
- *Employee access to long distance telephone lines*
- *Access to modem pool from remote telephones*
- *Authorizing prescriptions*
- *Electronic filing of income tax returns*
- *Access to patient's x-rays*
- *Access to databases*
- *Access to voice mail system*
- *Access to conference calls*
- *Access to long distance telephone lines*

5. CONCLUSIONS-RECOMMENDATIONS

In this chapter we draw conclusions from this report and some recommendations to users, evaluators and vendors.

No single biometric has dominated the market. Different technologies are used for the same applications. The current need in the biometric identification field is to have the market make greater use of what already exists.

The current generation of biometric identification devices offers cost and performance advantages over manual security procedures.

Careful evaluation of all mathematical tools (algorithms, protocols), software involved in the biometric technologies should be performed.

The security strength of the biometric methods should be proven. In particular the biometric methods should be tested against any cryptanalytic attack. Time and space complexity analysis should be performed on any successful attack, since as the computer power grows, theoretical attacks that are not feasible with the present computing power, will be successful in the near future. Such research should be undertaken by institutions whose expertise is to test the vulnerability of security systems.

The claims of systems designers need to be assessed by independent evaluators. The establishment of evaluation centers will bring the confidence that is missing today. An independent screening testing of all devices should be performed, i.e. treating the biometric devices as black boxes to examine how well the devices perform. These tests should be performed by independent institutions where manufacturers are not involved.

The lack of confidence for biometric technologies is caused by the lack of standards and testing. Standards will demonstrate that biometric technology is a reliable choice for providing security. They will give users from government and public sectors choice among the various biometric technologies, that will expand biometric market and it will make it competitive and trusty. It will also help manufacturers to evaluate their biometric products against standard tests. Different standardization bodies should cooperate in order to establish global standards. The ESPRIT project BIOTEST will be a milestone towards this direction since its main objective is to establish independent evaluative centers.

Product surveys on large sample of people should be carried out by independent companies in different countries. User's opinion is most important.

Criteria are required to be issued in order to evaluate the biometric methods and biometric technologies. A list of criteria is given in this report. Methods for testing against the biometric technologies should be developed.

As the number of application areas grow a concrete list of criteria should be formed by consortiums in each area. Such lists can be formed by independent companies following the next steps:

1. List all present and future application areas.
2. List major European organizations listed in application areas found in 1.
3. Send questionnaires to the IT management of all organizations formed in 2. asking them to list, describe their security infrastructure, grade their security priorities and software used for the effectiveness of their security management.
4. Analyze statistically the outcome of 3. Categorize and grade the priorities of each application area. List all existing security components that can be utilized by biometric technologies. Organizations like to reduce cost by using their existing facilities.
5. Form and grade criteria for choosing a biometric technology based on findings of 4.

Step 2 can be expanded to include international organizations so the derived lists will be more accurate and objective based on international needs.

Most biometric devices are still very expensive. It is unacceptable for a biometric device, used to protect a computer terminal, to cost almost the same as the computer itself. The cost will be reduced when the computer's CPU will be able to be used for storage and when the cost of lens and chip technology will be reduced.

The fear of "Big Brother" that the biometric technologies face can be overcome by various means:

- *use cards* to store the biometric templates whenever possible. The storage of templates in a central data base brings hesitation and discomfort. The Cascade project brought the development of smart cards capable to store biometric PINs. In case that biometric templates are stored in a central data base, they should be managed by a TTP whose trustworthiness is proven.
- *educate people* on the technologies. Most people are very skeptical of these technologies because they do not have significant information on them. There are several issues that bring hesitation which should be explained. For example it should be clarified that fingerprint technology is different than AFIS used to identify criminals. In the first, there is no comparison of fingerprints. People think that fingerprints are stored in the central data base, what is stored though are strings of 0's and 1's since they get encoded first.
DNA prints are used only to identify criminals. It should be made clear that justice is not interested in investigating and examining the genes and biological disorders of the individual. This is a different expensive process where biologists, doctors and specialist have to get involved in dedicated labs.
Educate people on the details of the biometric technologies. For example, the type of beams used in the iris or whole body analysis should be detailed described. Facts should not be hidden.

- *emphasize the advantages* of the biometric technologies. Counterexamples of fraud using the other authentication methods should be reported.
- *provide awareness* of when, how and where people are authenticated. People should know when and where they are identified and verified, and which technology is being used.

Storing the templates in a central data base is more economic than storing them in plastic cards. Unfortunately this method is lacking public acceptance. TTPs can provide the confidence that this method is missing by managing the templates in a trustful way.

Biometric devices are the future technologies since traditional technologies are not sufficient to reduce fraud and protect our computer systems and networks. It is naturally to use these technologies in various applications where security is the highest priority, e.g. Law enforcement, physical access control and banking. Securing sensitive data on the Internet is a popular concern. Internet banking and electronic commerce will be sectors where biometric technologies will provide a natural and logical solution.

Europe is the major player in the biometric technologies. European research institutes, and companies have developed biometric products. The European biometric market will expand if it is supported by R&D European projects. If Europeans use their own biometric products for their security needs then others will follow, and the European biometric market will be further stimulated and expanded.

ANNEX I: CRITERIA FOR BIOMETRIC TECHNOLOGIES

Criteria for Biometric Methods:

1. *Correct Algorithms*
2. *Secure algorithms*
 - *unconditionally secure*
 - *computationally secure*
3. *Good choice of keys* The choice of keys is important.
4. *Strong codes*
5. *Secure Data Base*
 - data base administrator should be proven trustworthy it.
 - template in data base should be securely stored, distributed and managed.
6. *Safe protocols*
7. *Secure Networks and Distributed Systems*

Criteria for Biometric Devices

1. OPERATIONAL

- *Convenient use:*
 - ◇ Minimum enrollment, authentication and verification time
 - ◇ Minimum user actions
 - ◇ Minimum user training
 - ◇ Minimum measuring and storing data
 - ◇ Minimum time to achieve recognition
- *Public acceptability:*

◇ User friendliness	◇ Physically and legally robust
◇ User security	◇ Familiar
◇ Ethical	◇ Private
◇ Not socially unpalatable	◇ Easy of use
◇ Conform to contemporary social standards	◇ Easy of counterfeiting an artifact
◇ Susceptibility to circumvention	◇ Reliability and Maintainability
◇ Compatible	◇ Resistance to deceit
- *Uniqueness* (the outcome should be unique)
- *Permanence* (the identifier should not change or be changeable)
- *Collectibility* (the identifier should not be collectible by anyone on any occasion)
- *Exclusivity* (no other form of identification should be necessary or used).
- *Human Factors*
 - ◇ Non intrusive (no physical contact with the identifier)
 - ◇ Non discriminatory (against: gender, age, physical and physiological condition, profession, imposed physical characteristics).
 - ◇ Suitable for the particular application (e.g. fingerprint is not suitable in environments where “hand free” is required).

2. TECHNICAL

- *Minimum Authentication Time*
 - ◇ User and system preparation time
 - ◇ Bio-data acquisition time
 - ◇ Matching Process time (verification time)
 - ◇ Measuring and storing time

- ◇ Memory size of the template
- *Low tolerance level*
 - ◇ Adjustable threshold settings for acceptance and rejection (depending on the security level required by the application).
 - ◇ False acceptance and rejection are low (Both Type I and Type II errors)
 - ◇ Self adaptive
- *Flexibility*
- *Strength*
- *Effectiveness*
- *Performance*
- *Standards (Compatibility, Interoperability)*
- *Storability (in manual and automated systems)*
- *Precision*
- *Simplicity*
- *Speed*
- *Independent of environmental conditions (noise, light, electromagnetic radiation, moisture, dust, temperature, humidity, smoke)*

3. FINANCIAL

- Equipment cost
- Installation cost
- Training cost
- Time and cost effort involved in updating
- Processing required involved in the computer systems to support the identification process
- Cost of protecting the device
- Cost of distribution and logistical support
- Interfacing of the device of its intended purpose
- Life-cycle support cost of providing system administration support and an enrollment operator.

4. MANUFACTURING

Support.

Exchange Data

REFERENCES

- [1] Adlrer, F.H. "Physiology of the Eye: Clinical Application, 4th ed., London: The C.V. Mosby Company, 1965.
- [2] Ahuja, V. "Network & Internet Security" Academic Press, NY 1996.
- [3] Anon. (ed.) "Colloquium on Electronic Images and Image Processing in Security and Forensic Science" IEE Colloquium (Digest), n. 087, 1990.
- [4] Ashbourn, J. "Practical Implementation of biometrics based on hand geometry" IEE Colloquium (Digest) n. 100, Apr. 1994.
- [5] Association of Biometrics "So you think biometrics may be the answer?" U.K., 1993.
- [6] Baltscheffsky P., and Anderson P. "Palmprint Project: Automatic Identity Verification by Hand Geometry" Proceedings 1986 International Carnahan Conference on Security Technology: Electronic Crime Countermeasures, 1986.
- [7] Betch, D. "DNA Fingerprint in Human Health and Society" Biotechnology Information Series (Bio-6).
- [8] Biometric Technology Today November 1995, vol. 3, n.7---October 1996, vol. 4, n.6, SJB Services, Soberest, England ([ht://www.sjb.co.uk](http://www.sjb.co.uk))
- [9] Bleha, S., Slivinsky, C, and Hussien, B. "Computer Access Security Systems using keystroke dynamics" IEEE Transactions on Pattern Analysis and Machine Intelligence, 12, no. 12, 1217-1222, 1990.
- [10] Bright, R. "Smartcards: Principles, Practice, Applications" New York: Ellis Horwood, Ltd, 1988.
- [11] Bryant, R. "Unix Security for the organization" SAMs, Publishing, 1994.
- [12] Burgess, S.P. "Law Enforcement Networks Puts Finger on Fast-Footed Criminals" SIGNAL, Oct. 1996
- [13] Caelliet, W. "Information Security Handbook", England, Macmillan Press Ltd, 1994.
- [14] Campbell, J., Alyea, L., Dunn J. "Biometric Security: Government Applications and Operations" <http://www.vitro.bloomington.in.us:8080/~BC/>
- [15] Carback, R. "Reducing Manpower intensive tasks through automation of security technologies" IEEE Annual International Carnahan Conference on Security Technology, Proceedings 1995, pp.331-339.
- [16] Chip Architecture for Smart Cards and Secure Portable Devices (CASCADE) Esprit Project EP8670, Data Sheet 1995.
- [17] Clarke, R. "Human Identification in Information Systems: Management Challenges and Public Policy Issues" Information & People, vol.7, no.4 (December 1994) pp 6-37.
- [18] Clinton, W.J. "Administration of Export Controls on Encryption Products (the "new Executive Order")", Novemebr 15, 1996.
- [19] Commission of the European Communities "Glossary of Information Systems Security "Contract 52001, Definitions within information systems security, 1993.
- [20] Cross J.M., Smith C.L. "Thermographic imaging of the subcutaneous vascular network of the back of the hand for biometric identification" IEEE Annual International Carnahan Conference on Security Technology, Proceedings of the 29th Annual 1995 International Carnahan Conference on Security Technology, pp. 20-35.
- [21] Daugman J. "High confidence Visual Recognition of Persons by a Test of Statistical Independence"
- [22] Daugman, J. "High confidence visual recognition of persons by a test of statistical independence" IEEE Transactions on Pattern Analysis and Machine Intelligence, v. 15, n. 11, Nov. 1993, pp.1148-1161
- [23] Davies, D.W. and Price W.L. "Security for Computer Networks" John Wiley & Sons, 1984.
- [24] Davson, H. "Davson Physiology of the Eye" 5th ed. London, Macmillan, 1990.
- [25] Deane F., Barrelle K., Henderson R., Mahar D." Perceived acceptability of biometric security systems" Computers & Security v. 14, n. 3, pp. 225-231, 1995.
- [26] Deming, R. "Dynamic Signatures for Personal Identity Verification" Proceedings 1986 International Carnahan Conference on Security Technology: Electronic Crime Countermeasures, 1986.

- [27] Denning, D. "Concerning Hackers Who Break into Computer Systems" 13 th National Computer Security Conference, Washington, DC, Oct. 1-4, 1990.
- [28] Diamond, S. "Biometric Security: What you are, not what you know" High Technology, Boston, 1987.
- [29] Ehrlich, T "Passports" Stanford L. Rev., v.19, pp.129--149, 1966-67.
- [30] FACFI (1996) "The criminal of false identification" federal advisory committee on false identification, Washington, DC, 1976.
- [31] Farley, M., Stearns, T. and Hsu, J. "LAN Times Guide to security and data integrity McGraw Hill, 1996.
- [32] Fejfar, A. and Myers, J.W. "The testing of three automatic identity verification techniques" Proc. International Conference on Crime Countermeasures" Oxford, July, 1977.
- [33] Feustel, T., Velius, G. " Speaker identity verification over telephone line: where we are and where we are going" Proc. 1989 Int. Carnahan Conf. Secur. Publ. by IEEE, pp.181-182.
- [34] Flom, L. and Safir, A. U.S. Patent No.4641 349, U.S. Government Printing Office, Washington, DC, 1987.
- [35] Fox-Davies A.C. and Carlyon-Britton P.W.P. " A treatise on the law concerning names and changes of name", Elliot Stock, London 1906.
- [36] Furnell, S.M., Morrissey, J.P., Sanders, P.W., Stockel C.T. "Applications of keystroke analysis for improved login security and continues user authentication" Proceedings of Information Systems Security (edited by S. Katsikas, D. Gritzalis), pp.283--294, 1996.
- [37] Galton, G. "Personal Identification and Description " Nature pp. 173-177, June 21, 1988
- [38] Garfinkel, S. and Spafford, G. "Practical Unix & Internet Security "O'Reill &Associates, Inc, Cambridge, 1996.
- [39] General Accounting Office "Electronic Benefits Transfer, Use of Biometrics to Deter Fraud in the Nationwide EBT program", USA, 1995.
- [40] George M.H., King R.A. " Robust speaker verification biometric" IEEE Annual International Carnahan Conference on Security Technology, Proceedings of the 29th Annual 1995 International Carnahan Conference on Security Technology, pp. 41-46.
- [41] Hamilton D.J., Whelan, J, McLaren, A. ,MacIntyre, I., Tizzard A. " Low cost dynamic signature verification system" IEE Conference Publication n 408 1995, England , p. 202-206.
- [42] Harmon, L.D., Khan, M.K., Lasch, R. and Ramig, P.F. "Machine Identification of human faces' Pattern Recognit., vol.13, pp 97--110.
- [43] Hays, R. "INSPASS" Jan 1996 <<http://www.vitro.bloomington.in.us>
- [44] HEW "Records, computers and the rights of citizens: Report on the secretary's advisory committee on automated personal data systems" (U.S. Dept. of Health, Education and Welfare), M.I.T. Press 1973.
- [45] Higgins, P. "Standards for the electronic submission of fingerprint cards to the FBI" Journal of Forensic Identification, The Official Publication of the International Association for Identification, vol.45, no. 4, 1995, pp.409-418.
- [46] Holmes, J. Wright, L., Maxwell, R. " A performance evaluation of Biometric identification Devices" Sandia National Laboratories, U.S.A, 1991.
- [47] IBM "Identification Techniques" IBM, 1969 (GC20-1707-0).
- [48] International Organization of Standardization, "Identification Cards-Physical Characteristics" Draft Proposal 7810
- [49] Jouce, R. and Gupta, G. "Identity Authentication based on keystroke Latencies" Communications of the ACM, 30, no.2, 168-176, 1990.
- [50] Kim, H.J. "Biometrics, Is it a Viable Proposition for Identity Authentication Access Control?" Computers & Security, 14, pp. 205-214, 1995.
- [51] King, R.A., Gosling, W. Electronics Letters , v. 14, n. 15, pp. 456--457, 1978.
- [52] Klopp, C. "More options for physical access control" Comput. Secur., v.9, n.3, May 1990, pp.229-232.
- [53] Konen, W. "Neural information processing in real world face recognition applications" IEEE Expert, v.11, n.4 Aug. 1996, p.7-8.
- [54] Lynch, M.R, Gaunt, R.G. "Application of Linear Weight Neural Networks to fingerprint recognition" IEE Conference Publication, n.409, 1995, pp.139-142.

- [55] Markowitz, J. "Speaker Verification, Who's there?" PC AI Intelligent Solutions for Desktop Computers, v. 9, n. 5, pp.24-26, 1995
- [56] Marsh, P. "Biometric Behavior is smart and secure" New Electronics, 9 July 1996, pp.25-26.
- [57] Maxwell, R. "The status of Personnel Identity Verifiers" Sandia National Laboratories, INMM Annual Meeting Proceeding, July 1985.
- [58] Maxwell, R., Wright, L. "Performance evaluation of personnel identity verifiers" Nucl. Mater. Manage, v.16, 1987, INMM 28th Ann. Meet., pp.417-423
- [59] Menezes, van Oorschot, Vanstone "Handbook of Applied Cryptography", CRC Press, 1996.
- [60] Mercer, J. "Design and strategies for optobiometric identification" Proceedings of SPIE-The International Society for Optical Engineering, v. 2659, 1996, p.60-66.
- [61] Mintie, D. "Biometrics in Human Services User Group Newsletter" vol.1, no. 1, July 1996 <<http://www.dss.state.ct.us/digital.htm>>
- [62] Morgan, D.P., Scofield, C.L. " Neural Networks and Speech Processing" Mass., U.S.A.: Kluwer Academic Publishers 1991
- [63] National Bureau of Standards "Guidelines on evaluation of techniques for automated personal identification" Federal Information Processing Standards Publication 48, 1977.
- [64] Newman, E. "The Biometric Report" SJB Services, UK, 1995.
- [65] Newton, J. " Reducing plastic counterfeiting " IEE Conference Publication n. 408, 1995, IEE Stevenage, England, p.198-201.
- [66] NZCS "Investigation of a unique identification system" N.Z. Comp. Soc., May 1972.
- [67] Parker, D.B. "A new framework for information security to avoid information anarchy" In Information Security -the Next Decade (eds. Ellof, J. and S. von Solms) Proceedings of the 11th International Conference on Information Security, IFIP'95, Chapman & Hall, London, 1995.
- [68] Partridge, C. " Success story that sounds familiar " The Times Tuesday May 28, 1996.
- [69] Rice, J. " Quality approach to biometric imaging" IEE Colloquium (Digest) n. 100, Apr. 1994.
- [70] Rohen, J. "Morphology and Pathology of the trabecular network in the structure of the eye", Smelser, Ed. N.Y.: Academic Press, pp. 335-341, 1961.
- [71] Rubenstein, H. "Time domain analysis yields powerful voice recognition" New Electronics, March 1994, pp.12-14.
- [72] Samal, A. and Iyengar, P.A. "Automatic recognition analysis of human faces and facial expressions: A survey" Pattern Recognit., vol.25, pp.65--77, 1992.
- [73] Schneier, B. "Applied Cryptography, Protocols, Algorithms and Source Code in C", J. Wiley and Sons Inc, Second Edition, 1996.
- [74] Scott, W. "Defense skills applied to biometric ID" Aviation week and Space Technology", v. 141, n. 16, p.54.
- [75] Sherman, R.L. "Biometric Futures" Computers & Security, vol. 11, no 2, Elsevier Science Publishers Ltd, 1992.
- [76] Sherman, R.L. "The right look can open doors" Security Management, vol. 36, no 10, Elsevier Science Publishers Ltd, 1992.
- [77] Sidlauskas, D. " A new concept in biometric identification 3-Dimensional Hand Geometry, Nucl. Mater. Manage, v.16, 1987, INMM 28th Annu. meet., pp.442-447.
- [78] Simonds, F "Network Security, Data and Voice Communications " McGraw-Hill, N.Y. 1996.
- [79] Spanish Government Agency Wins Outstanding Smart card Application Award at CTST'96 Awards Banquet. May 1996. CardFlash, RAM Research Group. <http://www.ramresearch.com/crdflash/cf5_20ohtml>
- [80] Stockel, A. " Securing data and financial transactions " IEEE Annual International Carnahan Conference on Security Technology, Proceedings 1995, pp.397-401.
- [81] Timms, S.R., King, R.A. "Speaker verification utilizing artificial neural network and biometric functions derived from time encoded speech (TES) Data" ICCS/ISITA Singapore 1992, pp.447--449.
- [82] Torbet G., Marshall I., Jones S. "Vital Signs for Identification" Computer Bulletin, v. 7, n.6, Dec. p. 14-15. 1995
- [83] Unisys Personal Identification Technology will be used to give Spaniers Access to Personal Information in Spain's Healthcare Databases. March 1996. UNISYS WORLD Editorial Index.

Publications & communications Inc.
<<http://www.pcinews.com/business/pci/un/editorials/spaniards.html>>

[84] Wambaugh, J. "The Bleeding" William Morrow, N.Y. 1989.

[85] What is NCIC 2000? NCIC 2000, vol.1, no 1, February 1996, Security Management Online
<<http://www.securitymanagement.com/library/000152.html>>

[86] Wood, H.M. "The use of passwords for controlled access to computer resources" National Bureau of Standards Special Publication 500-9, US Dept. of Commerce/NBS

[87] Zunkel, R. "Biometrics and Border Control" Security Technology & Design, May 1996, p.22-27.