"Acceptance Threshold's Adaptability in Fingerprint-Based Authentication Methods"

By

Mounina G. Bocoum

School of Computer Science McGill University, Montreal

July 1999

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements of the degree of Master of Science (M.Sc) in Computer Science.

Abstract

The individuals’ authentication is an necessary step in the securization process of any system including a person-machine interface. By being an automated process, it is essential that this authentication be based on infallible parameters, thus the interest for biometrics, as presented in this thesis. The study’s objective is to demonstrate the soundness of the threshold’s flexibility in biometric authentication systems. The emphasis is put on fingerprint-based methods. The hope is to promote the application of this kind of authentication, in areas such as electronic commerce and cellular telephony. Hence, this research paper starts by presenting the state-of-the art for both these domains. Then, the three existing authentication techniques are explained. The next step is the analysis of potential factors that will cause a threshold’s modification. Subsequently, for each of the selected criteria, a computation technique for the threshold’s new values is defined. A generalization of the threshold’s modification procedure is then exposed. The thesis finally closes, by an implementation of a part of the proposed generic procedure.

Résumé

L’authentification d’individus, constitue une étape incontournable de la sécurisation de tout système, présentant une interface homme-machine. Étant un processus automatisé, il est primordial qu’elle se base sur des paramètres d’identification infaillibles. D’où l’intérêt de la biométrie, comme démontré dans cette thèse. L’objectif de ce mémoire est d’établir le bien-fondé d’une certaine flexibilité, des seuils d’acceptation des systèmes d’authentification biométriques. L’emphase est mise sur les méthodes liées aux empreintes digitales. L’ambition est de promouvoir l’application de l’authentification biométrique aux domaines, tels que la téléphonie mobile et le commerce électronique. Le mémoire débute donc par dresser l’état de l’art concernant ces deux secteurs. Les trois techniques d’authentification existantes, sont ensuite exposées. L’étape suivante, représente l’analyse des potentiels facteurs de modification des seuils. Par la suite pour chacun des critères retenus, une méthode de calcul des nouvelles valeurs des seuils est définie. Une généralisation de la procédure de modification de ces seuils, est par la suite proposée. Enfin, ce mémoire termine par l’implémentation d’une partie de la procédure générique décrite.

Acknowledgements

I would like to express sincere gratitude to Dr Petre Dini for his guidance, his advice and suggestions in all aspects of the thesis and his encouragement. I thank him for always asking the best of me, in his subtle and humorous way.

I also thank Prof. Claude Crépeau for his interest in my work.

Special thanks and appreciation to the whole staff at CRIM, for welcoming me and improving my working conditions, particularly, Ms. Judith Bracke, Ms. Johanne Dumont.

Great recognition to Prof. Gerald Ratzer, for recommending me at CRIM.

Table of Contents

LIST OF FIGURES **7**

LIST OF TABLES **7**

INTRODUCTION **8**

CHAPTER 1: SECURITY NEEDS **10**

1.1 ELECTRONIC COMMERCE 10
1.1.1 Cryptography *11*
1.1.2 Electronic Cash *16*
1.1.3 Credit-card Applications *17*
1.1.4 Electronic Check *20*
1.2 CELLULAR TELEPHONY 21
1.2.1 Principles *21*
1.2.2 Cellular Fraud *22*
1.2.3 Solutions against Fraud *22*
SUMMARY AND TRANSITION 26

CHAPTER 2: AUTHENTICATION TECHNIQUES **27**

2.1 AUTHENTICATION BASED ON *KNOWLEDGE* 28
2.2 AUTHENTICATION BASED ON *POSSESSION* 29
2.3 *BIOMETRIC* AUTHENTICATION 30
2.3.1 Biometric Characteristics *31*
2.3.2. Problems encountered in Biometrics *47*
2.3.3 Adapting Biometrics to Electronic Commerce and Cellular Telephony *52*
SUMMARY AND TRANSITION 54

CHAPTER 3: POSSIBLE CRITERIA FOR THRESHOLD'S ADAPTABILITY **56**

3.1 FINGERPRINT FEATURES 58
3.1.1 Geographic distribution of the minutiae *58*
3.1.2 Minutiae's density *63*
3.1.3 Minutiae's Type *64*
3.2 APPLICATION NATURE 72
3.2.1 Commercial Application *72*
3.2.2 Level of Security *76*
3.2.3 Level of Privacy *78*
3.3 IMAGES OF POOR QUALITY 79
SUMMARY AND TRANSITION 81

CHAPTER 4: THRESHOLD COMPUTATION **82**

4.1 THE LEVEL OF SECURITY CRITERION 83
4.1.1 Fuzzy Logic: Principles *83*
4.1.2 Application on the Level of Security *87*
4.2 THE MINUTIA'S TYPE CRITERION 91
4.2.1 The "Rarity Weight" Variable *91*
4.2.2 A Possible Algorithm *93*
SUMMARY AND TRANSITION 97

CHAPTER 5: GENERIC METHOD FOR THRESHOLD'S ADAPTABILITY IN BIOMETRIC AUTHENTICATION SYSTEMS 98

5.1 THE PROCEDURE 98
5.1.1 The Feature and its Representations 99
5.1.2 The Choice of G 101
5.1.3 The EVAL() Function 103
5.1.4 Threshold 118
5.1.5 The Procedure's Schematization 121
5.2 A FURTHER CONSIDERATION 123
SUMMARY AND TRANSITION 125

CHAPTER 6: SIMULATIONS/IMPLEMENTATIONS 126

6.1 THE CONCEPT 126
6.2 THE ANALYSIS 127
6.3 THE IMPLEMENTATION DETAILS 128
6.3.1 The Generic Class (Main) 128
6.3.2 The Tab Class 129
6.3.3 The Minutia Class 129
6.3.4 The ExceptionC Class 130

CONCLUSION 132

REFERENCES 134

List of Figures

FIGURE 1: ENCRYPTION OVERVIEW 15
FIGURE 2: TOPOLOGY OF BIOMETRIC IDENTIFICATION METHODS 31
FIGURE 3: MINUTIAE DETECTION 37
FIGURE 4: IMAGE ENHANCEMENT 40
FIGURE 5: MATCHING SAMPLES OF THE SAME PERSON 42
FIGURE 6: MODEL OF AUTHENTICATION METHODS 49
FIGURE 7: BEFORE ORIENTATION ESTIMATION 60
FIGURE 8: AFTER ORIENTATION ESTIMATION 60
FIGURE 9: AN ARCH COMPARED TO A LOOP 61
FIGURE 10: FEATURES OF THE MEMBERSHIP FUNCTION 85
FIGURE 11: FUZZIFICATION OF THE TEMPERATURE CONCEPT 85
FIGURE 12: DEFUZZIFICATION 86
FIGURE 13: LEVELS OF SECURITY MEMBERSHIP FUNCTIONS 89
FIGURE 14: MINUTIAE NUMBER MEMBERSHIP FUNCTIONS 90
FIGURE 15: THE ORGANIZATION OF *G* 101
FIGURE 16 : IMAGE ANALYSIS 104
FIGURE 17: THE HIERARCHICAL IMAGE PYRAMID 106
FIGURE 18: SELECTION OF POTENTIAL RELEVANT REGIONS 112
FIGURE 19: CORRECT MODEL (COORDINATES OF THE ELEMENTS, WITH THE NOSE AS THE REFERENCE) 116
FIGURE 20: CORRECT MODEL (THE LEFT EYE IS THE REFERENCE) 117
FIGURE 21: GENERIC PROCEDURE DIAGRAM 122
FIGURE 22: ENTITIES AND RELATIONSHIPS 128

List of Tables

TABLE 1: COMPARISON OF BIOMETRIC TECHNOLOGIES [] 44
TABLE 2: AUTHENTICATION METHODS COMBINATIONS 49
TABLE 3: COMMON MINUTIA TYPES [28]..... 65
TABLE 4: GRADING OF MINUTIA TYPES OCCURRENCES..... 67
TABLE 5: THRESHOLDS CHOICE IN AFIS X..... 77
TABLE 6: MINUTIA TYPES' WEIGHTS 92

Introduction

The necessity for human beings to be able to authenticate and identify each other is a feeling inherent to individuals' relationships. "To know with whom one is confronted" constitutes the foundation of confidence establishment. This demeanor is present at all levels of our life, from social relations to civil recognition. In our world leading to "machines' domination", this concept is even more meaningful, as non-human entities tend to be necessary intermediaries in human interactions. Therefore, it is absolutely required to correctly identify our interlocutors. In our obsession of transforming our planet into an interplanetary village, with the proliferation of all types of networks, people are in less and less "palpable" contact. The obvious advantage of this tendency is the priceless freedom it gives us to communicate. One of its drawbacks, is the obligation to conceive automatic methods for authentication, not requiring human presence.

Various methods for such a purpose have been imagined and implemented. This study will focus on one of them: the authentication based on *biometrics*. "*The statistical analysis of biological observations and phenomena*". The real expectation of this topic is, eventually, the use of biometric authentication as a technique to secure areas such as, electronic commerce and cellular telephony, extremely promising commercially.

However at this point, this thesis has a more restricted and prosaic goal. It aims at establishing the validity of the "flexibility" concept in automatic biometric authentication systems. Flexibility in the sense that the systems should be made adaptable to various conditions of identification, concerning both the changes that can occur at the users' biological characteristics level, and the changes resulting of external situations.

Chapter 1: Security Needs

The number of Internet users by the end of 1998 was estimated at around 147 millions and is expected to rise to 320 millions by the end of year 2000 [1]. From a financial point of view, the Internet represents an inestimable gold mine for companies worldwide, whatever their size or capital. Especially with electronic commerce as a way of raising companies' market to an international level. However, the main obstacles to the full establishment of this type of commerce are the "*Security risks associated with sending unprotected financial information across public networks*", as well as *"the anonymous nature of the communications networks*" [2]. This justifies the usefulness of the authentication procedure, to precisely identify the actors in electronic transactions. Associated with other techniques, like cryptography, it will improve the security and the information privacy, to make the public less defiant to this form of business.

In the mobile telephony world, the fraud costs "*the cellular industry approximately $1 million dollars a day*"[3]. It represents *"the fastest growing telecom fraud*"[4], and takes diverse forms, from the simple steal of the phone to the impersonation of the customer. The authentication of a genuine user, prior the use of the phone, will help to prevent this costly type of swindle.

1.1 Electronic Commerce

Commerce over the Internet tries to establish the same relations with the clients, than the "face-to-face" one has with them. Merchants are grouped together by categories, on web sites called "commercial windows". Those windows can be interpreted as electronic malls. Payment methods are similar to the existing ones, namely cash, checks, or credit cards. The only thing missing is the possibility of weighing up and evaluating the goods with naked eye. However, it is compensated by the convenience of shopping from home. Another dissimilarity is the impossibility for the users to buy anything from any merchant on the web. Generally, the clients would be allowed to do business only with merchants within their community. The electronic services' provider defines the community. This is due to the fact, that there isn't one standard determined and used. Consequently, every provider applies a particular solution with a certain number of merchants and clients.

In the following section, in order to have a better understanding of how the fraud is conceivable, a description of the payment methods, utilized in electronic commerce, is given. But first, a small tutorial on cryptography, widely used in electronic commerce, follows.

1.1.1 Cryptography

The cryptography "science" is used to protect private information from unwelcome persons, by encrypting the data. However, as a whole, it embraces other technologies such as digital signatures and certificates.

1.1.1.1 Encryption

Cryptography is the technology that encrypts a message, using a key and allows only the holder of the appropriate key, to decrypt this message to recover the original one. Cryptography is particularly useful in open systems environments, where networks are not safe enough to securely transmit information. There are two ways for encryption-decryption: the symmetric or *secret-key* cryptography and the asymmetric or *public-key* cryptography.

Secret-key cryptography uses the same key (symmetric) to encrypt and decrypt a message. Therefore, this key must be kept "secret". Only the sender and receiver of the message should possess a copy of it. Data Encryption Standard (DES) is an example of a well-known secret-key cryptography algorithm used by financial institutions to encrypt Personal Identification Numbers (PIN) [2].

Public-key cryptography employs two different keys: a public key to encrypt messages and a corresponding secret key, to decrypt the messages from the related public key. Each user of the system posseses both a public and a private key.

The public key can be largely distributed because it is only used for the encryption of messages to the owner of the secret key. Both keys are mathematically related to allow the decryption, however, if the system is correctly designed and implemented, it is impossible to derive the secret-key from the public-key. With two users involved in a transaction (users A and B), when both want to send encrypted messages to each other, they both have to send their respective public keys to the other one. A will use B's public key to encrypt messages for B, who will use his/her private key to decrypt those messages and vice versa. An example of a known public-key cryptography algorithm is RSA (named after its inventors, Rivest, Shamir and Adleman).

1.1.1.2 Digital Signatures

Digital signatures are the electronic application of handwritten signatures. However, the aim of digital signatures is twofold: the authentication of the message sender and the verification of the data integrity. Digital signatures may apply public-key cryptography. Indeed, each key of a public-key cryptography system can be used in two manners:

The secret key is utilized to decrypt messages issued by an owner of the corresponding public key or to sign (create the digital signature) transmitted messages. The public key can encrypt messages and read (verify) the signature created by the owner of the related secret key.

- **The digital signature creation**: the message to sign is passed through a mathematical function (hash function) to produce a hash value. A hash value is a smaller version of a message (easier to manage), yet, unique to the corresponding message. Indeed, a change to the message will result in a change of the hash value if using the same hash function[]. However, several messages can have the same hash value, because of its small fixed length that cannot permit a hash value, unique to each message.

The hash value is then signed using the sender's secret-key. This encrypted hash value, the digital signature, is eventually appended to the original message and the whole information is sent.

- **The digital signature verification**: The receiver verifies the digital signature by using the public key, corresponding to the sender's private key. If the operation succeeds, it ensures that the hash value was signed by the correct sender. The receiver of the message then recomputes the hash value of the original message, with the same hash function used by the sender. Finally, both the newly computed hash value and the one obtained after verification of the digital signature, are compared to check the message integrity.

1.1.1.3 Certificates

With digital signatures, users know that the messages they receive indisputably come from the senders of the corresponding public keys, unless an assumption is broken. Prior to that, receivers must authenticate these senders. This is accomplished with *certificates*. An authentication certificate is delivered by a "Certificate Authority"(CA)[1], to testify to people's identity. Certificates are composed of the users' identification information as well as their public keys. The Certificate Authority digitally signs it, after it has successfully verified the user's identity. With this certificate, a user is able to prove the ownership of a public key, and has to distribute it (the certificate) to the other users before the initiation of the first transaction. The receiver will compare the sender's public key with the one in the corresponding certificate.

---

1 "*A Certificate Authority might be an external company such as VeriSign that offers digital certificate services or they might be an internal organization such as a corporate MIS department." The Certificate Authority's chief function is to verify the identity of entities and issue digital certificates attesting to that identity*". (FOLDOC at http://wombat.doc.ic.ac.uk/foldoc/index.html)

Figure 1 shows a typical transaction between two users using encryption for message exchange. All the techniques explained above are utilized in this transaction.

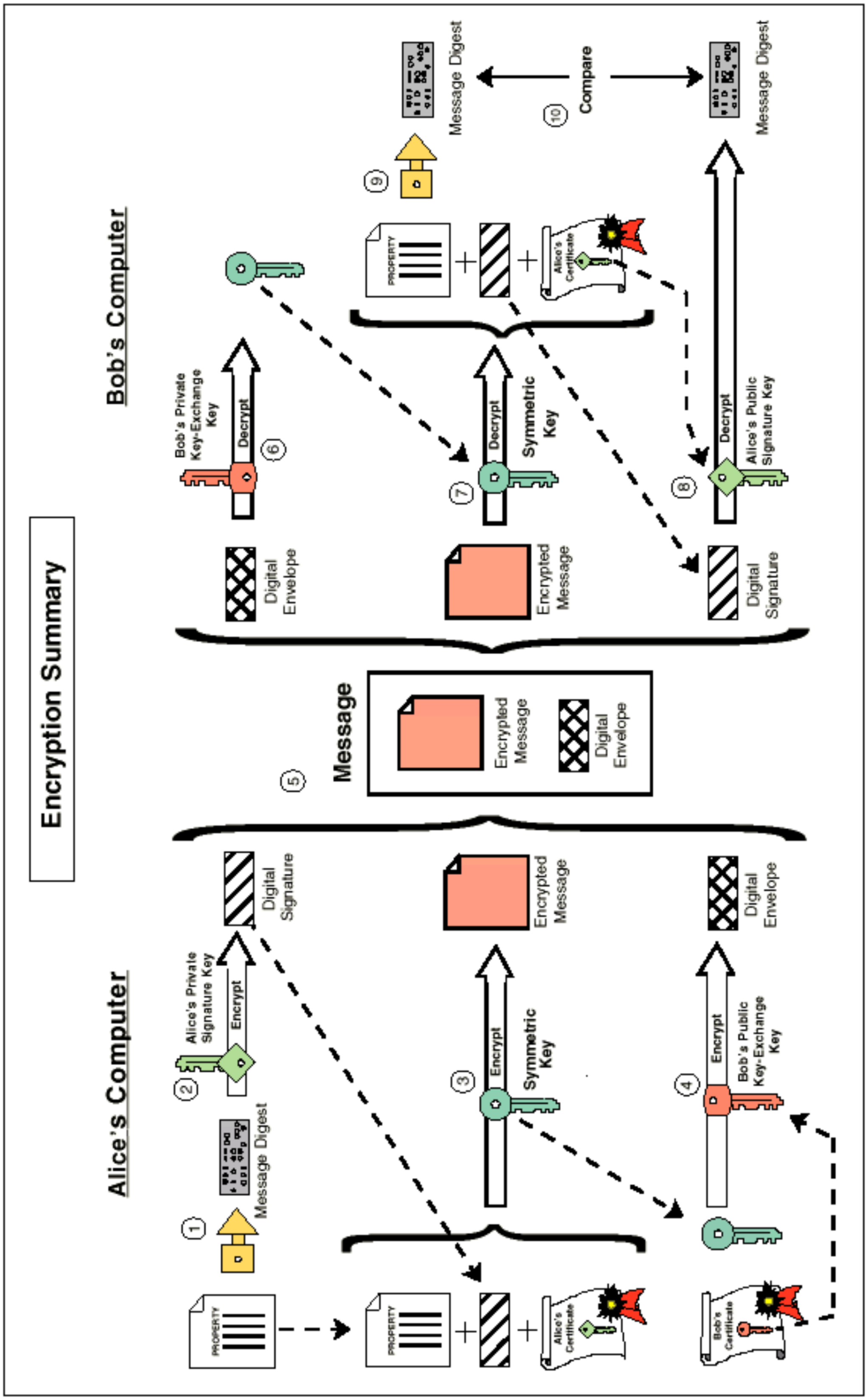


Figure 1: Encryption Overview [2]

1.1.2 Electronic Cash

Generally, most of the systems implementing electronic cash, present similarities in their characteristics. They rely on the existence of a "cyberwallet", or an item that has the same functionality, to store electronic money retrieved from the customer's bank account. Some systems just mention that the money is stored on the client's hard disk, however in my opinion, it is comparable to a wallet, even if it is not named so. This cyberwallet resides on the clients' computers. To ask the banks to fill their wallets, clients send them encrypted messages, digitally signed, with the requested amount. Banks decrypt the messages with their private keys and check the signatures. They then, deduce the amounts from the clients' bank accounts and "transform" the money in "*serial numbers*". Those numbers are encrypted, signed and sent back to the clients, who store them in their wallets for further uses. To pay the merchants, the clients send them messages containing the amount of money due. The merchants then contact the banks to make sure that the serial numbers corresponding to the electronic cash haven't been spent elsewhere. The banks can, at this point, credit the merchants' accounts [5]. As the electronic money corresponds to serial numbers, a replay scenario won't succeed. Before a payment is acknowledged, the bank checks if the serial numbers haven't been already used. Companies such as CyberCash with *CyberCoin* [6] or Digicash with *Ecash* [7] have applied this technology.

Another method adds a hardware device to the transaction: a smartcard. This involves a new hardware to buy both for the clients and the merchants (a smartcard reader) to be able to use this smartcard from home for purchasing over the net. This is the solution conceived by "Mondex". To pay for something on the Internet, users simply have to insert their cards in the readers to send the payments to the merchants' Mondex cards. The protocol used for the transactions employs encryption and digital signatures to enforce security. The smartcards can be reloaded from home or at an Automated Teller Machine (ATM) (when the banks integrate this technology). The electronic money is directly transferred from one chip to another [8].

The manipulation of electronic cash is really convenient for "micropayments". "*Micropayment are transactions that range from 1/10 of a cent to $10.00 and up* [5]. "*Used where the service is metered out and charged on very small increments, e.g. traditional telephone charges, new automatic toll charges and other digital cash applicatio*ns" [9]. Users might be reluctant to use their credit card each time they have to pay for small amounts of money over the Internet. It is even more unpleasant for merchants who are sometimes charged when their customers pay by credit cards. Therefore, electronic cash is the perfect answer to this issue. However, one of the noticeable drawbacks of this payment method is, the necessity for both the clients and the merchants to subscribe first to a particular provider in order to use the electronic cash system. They are then exclusively restricted in their transactions to members of this "virtual community".

1.1.3 Credit-card Applications

As the most widespread payment method nowadays for commerce, it is not surprising that the credit card is also the most popular solution chosen by consumers for online commerce.

1.1.3.1 Description

Credit-card applications don't require any transaction with the bank or any additional hardware device. Many web sites provide secure protocols to allow reliable transmission of the clients' credit cards information over the Internet. Protocols like *SSL* (Secure Socket Layer)[2] and *S-HTTP* (Secure Hypertext Transfer Protocol)[3] encrypt messages to prevent eavesdropping.

2 A protocol designed by Netscape Communications Corporation to provide encrypted communications on the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, Telnet, FTP, Gopher, and NNTP and is layered above the connection protocol TCP/IP. It is used by the HTTPS access method.

3 S-HTTP is an extension to the HTTP protocol for secure transmission of data over the WWW. The difference with the SSL protocol is that : "*S-HTTP is designed to send individual messages securely,*

With credit card applications, clients are not limited by community membership, as in the E-cash approach. They can buy goods and services at any web store that includes this feature. However, the inconvenience is that, the credit card information is transmitted at each purchase. It increases the chances for hackers to succeed in breaking the encryption key. To ward off this danger, clients can choose to become affiliated to an intermediary, in order to provide only once the "sensitive" information, at the registration. At this time, the credit card's information don't have to be transmitted by the network. They can be communicated by telephone, fax or any other communication medium. The customer is then assigned a username and password, used for shopping at merchants also affiliated to the same intermediary. The community membership's notion appears here again.

When the clients confirm a purchase, the intermediaries debit their credit cards to credit the merchants'. Companies like FirstVirtual, OpenMarket [10], NetMarket [11] have implemented this approach.

A third procedure is the reuse of the notion of "cyberwallet" to store the multiple credit cards of a customer. At each order, the client chooses one card for the payment. The order and the credit card information are then sent over the net, encrypted to the merchant. This one keeps the order's information and transmits the financial information (credit card), still encrypted, to the bank. This merchant's bank will then contact the client's bank to equilibrate the accounts. This procedure is the solution of CyberCash [12].

With credit cards, as soon as an impostor can obtain the credit card information of a customer, the replay scenario is possible. When the card information are transmitted at every purchase (without the affiliation to an intermediary), as long as the cards' owners don't become aware of their cards' utilization, there is no way to detect the fraud. Even with an intermediary, knowing the login and password used for the connection, is enough for an impostor to purchase goods over the Internet, using the card of a genuine user.

---

whereas SSL is designed to establish a secure connection between two computers." ("PC Webopaedia Definition and Links" : http://webopedia.internet.com/TERM/S/S_HTTP.html)

1.1.3.2 The SET Protocol

With the great economic potential that electronic commerce carries, a single and common specification, set by competent and trustable institutions (for a better public acceptance) was required. Visa and MasterCard have joined their efforts to come up with a standard, concerning credit card applications, released to the public in 1997. A standard, that hopefully will bring security in the transactions and will be used for most of the online transactions. It was developed in collaboration with GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa and Verisign. The Secure Electronic Transaction (SET) [2] protocol was developed with the idea that an Internet user should be able to buy things over the network without revealing to the other transaction's actors (merchants and banks), the information they don't have to know. Clearly, merchants don't have to see the clients' credit cards and banks don't have to know what clients do order. The SET protocol should allow a reliable, "discreet" online transaction. To reach this goal, the protocol objectives are:

– The actors authentication (cardholders and merchants)

– The data confidentiality (credit card information)

– The data integrity (information shouldn't be altered during transmission)

Therefore, SET employs different aspects of cryptography to fulfill these objectives:

– Digital signatures and Certificates (both for cardholders and the merchants) permit the actors' *authentication*.

– Message encryption guarantees the data *confidentiality*

– Digital signatures also serve for the information *integrity*.

The SET protocol shows great promises as a consensus for the development of electronic commerce and if well accepted, should replace gradually the SSL protocol for web-related transactions.

1.1.4 Electronic Check

Checks have less success than credit cards among the public, however they are still largely in use in the financial sector. Therefore, research has also been done in this area, for electronic check. An electronic check contains the same data as a paper check. A stronger signature replaces the handwritten one: a digital signature that can be checked at any step of the transaction. All the other information are indicated (payee's name, amount of the transaction, account information, date).

The Financial Services technology Consortium (FSTC) has created the *echeck* [13], to be the exact replica of the paper version. Everything is similar, except the fact that papers disappear. The transaction's flow remains the same. The payer writes an echeck, "*cryptographically signs*" it (using digital signatures) and sends it to the payee. The payee verifies the signature (thanks to certificates issued for public key verification) and digitally endorses the check. The check is then transmitted to the payee's bank, which ascertains both signatures before crediting the payee's account. Finally, the check is forwarded to the payer's bank to debit the corresponding account. The echeck is written in a particular language (the Financial Services Markup Language). The checkbook is represented by a smartcard. This password-protected card contains the payer's private signature. The only use of cryptographic signatures is sufficient to prevent frauds with echeck. The check itself doesn't have to be encrypted when sent. Because of all the security techniques employed (authentication, public key cryptography, digital signatures, certificate authorities, duplicate detection, encryption), the echeck can be sent by any communication medium (email, the Internet or other network services). It is a simple document that can be implemented by any application. To avoid replay with the echeck, the electronic checkbook automatically numbers each echeck before it is signed by the payer. The payer's bank when receiving the check, verifies that it is not a duplicate. Finally the transaction appears on the payer's statement with all the information contained on the echeck, therefore, he will notice a possible error.

CyberCash keeps the same approach as before and uses the cyberwallet as a checkbook also. The transactions here are encrypted. The software is password-protected and maintains a transaction log [12].

Electronic cash, credit cards and electronic checks compose the three existing modes of money transactions over the web. To enforce security, they only dispose of cryptography techniques, which are rather complex. Moreover, despite this security feature, they are still not entirely safe from frauds, at the moment.

After the electronic commerce, the cellular phone world is another domain that necessitates security, due to the rising number of frauds perpetrated. Here is a brief description of the types of frauds and the solutions used against them, for now.

1.2 Cellular Telephony

To be able to understand the mechanisms of frauds for cellular phones, a brief explanation of the system's concept is required.

1.2.1 Principles

A cellular phone is distinguished from another phone by a pair of identification numbers: an Electronic Serial Number (ESN) and a Mobile Identification Number (MIN). "*The ESN is hardwired by the manufacturer and the MIN is programmed by the provider*"[14]. The ESN identifies the phone itself, whereas the MIN identifies the customer and the cellular provider. An electronic component found on every phone binds the MIN and the ESN, which are continuously transmitted over the air to the nearest cell site, as long as the phone is turned on [3]. The cell site then forwards the information to the subscriber's home switching office, for validity verification.

1.2.2 Cellular Fraud

There are four ways of committing fraud using a cellular phone [14]:

– *Theft* (the most common)

– *Subscription fraud*: the thief uses a fake or genuine user's personal information: name, address. The person is then able to use the phone until the contract is rescinded for lack of payment. It can take from one to three months.

– *Cloning* (2 types): The cloning of a cellular phone consists in using a genuine user's account to make calls [14]. This user's ESN/MIN pair can be stolen when transmitted in the air. There are two modes of cloning:

- Tumbling: in a "tumbler phone" a chip is installed that chooses at each call a different ESN/MIN pair. These pairs can be false or valid pairs. They take advantage of a weakness of the cellular system: when the pair ESN/MIN is communicated to the cell site, at each call this cell site forwards the information to a switching office. This office checks among a fraud database if the pair ESN/MIN is valid. If it appears on the fraud list then the next call will be denied but the current one succeeds. Thus, as the identification numbers change at every connection, they are hard to detect.
- The other type of cloned cellular phone is phone tampered with a legitimate ESN/MIN pair. To read those numbers in the airwaves, thieves use equipment utilized by the cellular service providers.

In front of the tremendous expansion of the frauds in this sector, techniques have already been implemented to try to solve this costly issue.

1.2.3 Solutions against Fraud

Several methods have been developed or are currently studied, against cellular fraud:

– *User verification*: PIN can be used to lock and unlock the phone. It prevents its use when the phone is stolen, as well as the theft of ESN/MIN pair, which can be intercepted only when the phone is unlocked.

– *Signals Encryption* against the steals of ESN/MIN codes.

– *Traffic pattern analysis*

– *Blocking*: certain "high-risk" subscribers will be denied certain types of calls (ex: international calls will be allowed only with major credit cards and the assistance of an operator) [14]

– *Authentication* (biometrics and other)

– *Radio Frequency (RF) Fingerprinting Technology*

Here follows a presentation of each of these countermeasures.

1.2.3.1 Encryption

With encryption, it is difficult for hackers to decrypt the ESN/MIN pairs in the airwaves. Moreover, it prevents communications eavesdropping. It is possible but not easy to encrypt analog signals, as a result, digital cellular phones are favored for encryption. The series of 1's and 0's are more suitable for cryptography. The emergence of the new generation of wireless phones on the market, the Personal Communications Services (PCS) phones, promotes the encryption usage. Even though, analog phones remain the most common. However, encryption is not well perceived by governments. In the United States, governmental organizations, like the Federal Bureau of Investigation and the National Security Agency are opposed to its development in the cellular world. They fear that criminals and terrorists will take full advantage of this feature [14].

1.2.3.2 Traffic Pattern Analysis

This method is not only widely used for cellular phones, but also in the whole telephony industry [14]. It aims at detecting unusual behavior for a particular subscriber. It works in general with artificial intelligence software. Each subscriber has a general "calling conduct" and when software detect calling patterns which are not in accordance with the user profile, they signal it. It may be an unusual number of international calls or an increase in the communications length. They can also verify if a call is "physically" possible, depending on the previous call made. Some products already exist for traffic analysis: *FraudBuster®* and *ChurnAlert* both developed by Coral Systems or *CloneGuard* by Electronic Data Systems and Pacific Telesis. The major drawback of solutions based on profiling analysis is that by the time the fraud is detected, the call has already been made.

1.2.3.3 Authentication

- *Voice verification*

Authentix Roamer Verification Reinstatement (RVR) authenticates the user of a phone. To be able to utilize their phones, users have to identify themselves by voice verification. At a call attempt, the call is transmitted to a verification center and the users have to provide a code only known to themselves and the subscriber. The verification takes about 18 seconds to complete [3].

- *Authentication methodology*

The authentication method used here is only efficient against cloning. It will not prevent a thief to use the phone. It verifies if the ESN/MIN pair issued by a phone really belongs to it, thus excludes cloned phones. The system lies on a challenge-response mode. When a call is started or received, the phone receives a challenge from the Authentication Center (AC). It then generates a response with the ESN/MIN pair and a secret key, and sends it encrypted to the AC for verification. The AC compares the response with the one that should correspond to this particular phone. If they don't match, the call is denied.

The North American Cellular Network (NACN) has developed its own authentication protocol [15]. It works with an authentication key (A-Key), a secret value unique to each cellular phone. Only the phone itself and the AC hold a copy of this A-key. It is never transmitted through the air, unlike the ESN/MIN pair. The key can be manually programmed in the phone, either by the user or by the manufacturer. When the phone is used, whether to receive or establish a call, the AC issues a random number to the phone. The phone then uses this random number, the A-key, the ESN/MIN pair and the CAVE (Cellular Authentication and Voice Encryption) algorithm to calculate the response to this challenge. The AC uses also those data to generate the response and compares it with the one given by the phone.

1.2.3.4 RF Fingerprinting Technology

This technology is based on the fact that cellular phones send radio frequency (RF) signals whenever they're on. Those patterns of RF signals differ from a phone to another, even for the same model. A cellular phone's RF fingerprint is "*the mobile ID number or electronic serial number, a measurement of several different features of the wave form center frequency deviation*" [3]. Clones can be detected by comparing the RF signals they broadcast with the ones of the legitimate "owner" of the ESN/MIN pair. The advantage with RF fingerprinting is that fraud can be detected in real-time and phone calls stopped at this moment [3].

" *The process of receiving the signal, measuring its RF fingerprint and comparing the print to the database takes about _ second* " with Corsair Communications' *PhonePrint* system.

Surprisingly, all these various solutions are not sufficient for efficiently countering the impostures, given the loss of profit related to frauds, in this industry.

Summary and Transition

The key word in electronic transactions and communications by cellular phones is ***SECURITY***. This is the *only* obstacle that should be overcome. Once this question is solved, in a satisfying, confident, consensual manner and is perceived in such a way by the public, then electronic commerce will explode.

Of course, there'll never be ONE everlasting solution to prevent frauds. There will always have people to break those security barriers and it's a process that evolves perpetually. But a starting point should be found, to promote and launch such a practice among users.

The question raised here is "How to secure domains like electronic commerce and cellular communication business?" What does "secure" mean? The first consideration is the integrity of the data sent over the networks. The second, in which this discussion is more concerned, is the insurance that clients only pay for what they have ordered (or consumed, in the telephony world), that merchants get those payments and finally that clients actually receive the correct orders. There is one way to achieve this goal, is to succeed in accurately ***authenticating*** the people involved in the transactions.

Chapter 2: Authentication techniques

The authentication process is used to verify a person's identity. It is an intrinsic property of security, especially in computer systems. It answers the question "Are you really who you claim to be?" It is a fundamental component of electronic commerce and cellular communication.

In the cellular communication domain, it is the solution against frauds. If it's feasible to prevent impersonation of customers, then it will dramatically reduce the financial losses.

The crucial issue in electronic commerce is twofold: the safety of the data exchanged over the net and the authentication of both the clients and the merchants. How to ascertain the identity of the client to charge? The identity of the person who pays for the goods or services?

The problem concerning the protection of the data sent is solved with the existence of standards, like the "Secure Electronic Transaction" (SET) protocol, which ensures data integrity. This aspect will not be treated in this paper; it will rather focus on the user's authentication.

There are three ways to authenticate a person. By asking the users:

1. Something they know: *Passwords*
2. Something they have: *Smartcards*
3. Personal characteristics: who they are: *Biometrics*

All these methods are at different levels of their "life cycle", in their recognition and utilization by the public.

2.1 Authentication based on *Knowledge*

This first solution is companies' first choice for users authentication. The vast majority of computer systems in companies are set up with password-based authentication. It is certainly a fast solution for authentication and above all the cheapest, but it is also the simplest to hijack. In open network environments, it is very easy to eavesdrop passwords sent in clear and reuse them later to impersonate legitimate users. These attacks are called "replay attacks".

Cryptography has been added in such environments to bring robustness. Kerberos [16] is the most commonly used system of authentication based on cryptography. It has been developed by the Massachusetts Institute of technology (MIT). *"Kerberos is a distributed authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or just a server) without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal*" [16]. Kerberos uses the Data Encryption Standard (DES), a secret-key encryption algorithm, to encrypt its messages. It only works for messages exchanged between software, which has been modified to implement it. Still, like most password-based systems, it remains weak in the face of the "guessable" character of passwords. Particularly when considering how users choose their passwords in the real world. Moreover, in large systems the password solution may be hardly manageable, because of the numerous passwords required for each subsystem.

An answer to password guesses and replay attacks is "One-Time Passwords". Those passwords are only valid for one connection. Consequently, even if attackers succeed in finding them, they will not be able to impersonate the user, as the next connection will require a new password.

Guessing a password is a passive attack; the attacker just tries to find the password of legitimate users to impersonate them. The impostor will penetrate the system with valid data. By opposition to an active attack where the attacker tries to break the system to enter it, or tries to find a way to circumvent it. This can be seen as a “brutal attack”. Active attacks are of course, easier to detect than the passive one, as in the later case if nothing is altered in the users’ accounts, they will not know that someone else possesses their passwords. Kerberos is mostly efficient against active attacks, whereas a one-time password scheme is preferable against passive attacks and will not prevent the first type. Another solution that will be efficient against passive attacks, is "Zero Knowledge Proof". This type of interactive proof involves a "prover" and a "verifier". The idea is for the prover to persuade the verifier of a statement, without revealing any information about how to obtain this statement [17]. Applied to authentication, it means that a registered user will convince the system of his identity, without giving anything that somebody could use to impersonate him. Still, against active attacks, this method won't be efficient.

Passwords are currently used in many credit card applications. When users registered to an intermediary, they have to provide their login names and passwords to shop on the Internet, for the payments.

Concerning cellular phone, password-authentication is also applied to prevent a thief from using a stolen phone. The owner locks and unlocks the phone with a PIN to have access to its functions.

An alternative to password-based authentication is the one based on *possession*.

2.2 Authentication based on *Possession*

A smartcard is a plastic card, the size of a credit card, integrating a microchip. A smartcard is a kind of miniature computer. The chip is a real processor with memory, to store data. The superiority of smartcards over magnetic stripcards is that they not only store data, but they can also perform computations to protect them. Several levels of “intelligence” can be found in the cards, allowing them to control the access of the data they hold. Encryption can be used to protect those data, for example to prevent impostors from eavesdropping them, when they are transmitted over the network. Passwords and PIN can be required from the user, for the card to release the requested information. As well as biometric verifications to ensure that only the card owner will be able to use it. Smartcards add a level of security because, to authenticate themselves, users not only need to hold a card, but also need to provide additional information (PIN or a biometric characteristic). The fact that the smartcard is a hardware device makes it more difficult to attack than software. "*An important and useful feature of a smart card is that it can be manufactured to ensure the security of its own memory, thus reducing the risk of lost or stolen cards*" [18]. However, here also, even when the smartcards use is reinforced with a password system, for an impostor to penetrate the system, it is "sufficient" to hold the card and have the PIN. The only really efficient approach is the use of smartcard and biometrics. The card can be used exclusively by its owner, as the biometric characteristics are unique to individuals.

Biometrics is the last existing authentication method. It can be used alone, without smartcards. Hence reducing the cost of authentication systems.

2.3 *Biometric* Authentication

Biometrics authentication is used since the nineteenth century, long before the emergence of "modern computing", to identify individuals for forensic purposes. However, as the most "natural" way of identifying individuals, (simply by recognizing their faces or other biometric traits, like their voices), it can be considered as the oldest mode of authentication. Several physiological and behavioral characteristics of a person are known to be unique, indeed favoring their uses as ways of authenticating a person. By exposing "who we are", it is assumed that it will lessen the opportunities of impersonating someone. Fundamentally it should be considered more secure than other authentication methods such as the "what you know", approach where users have to submit passwords, over a network, which are not safe from eavesdroppers. Biometrics has been widely used in forensic, in criminal issues, but it is now applied in a wide range of areas, such as banking, access control, ID systems, etc. Even if this approach is "the most natural" and surely the first one to be thought of, it is confronted with many technical and structural problems.

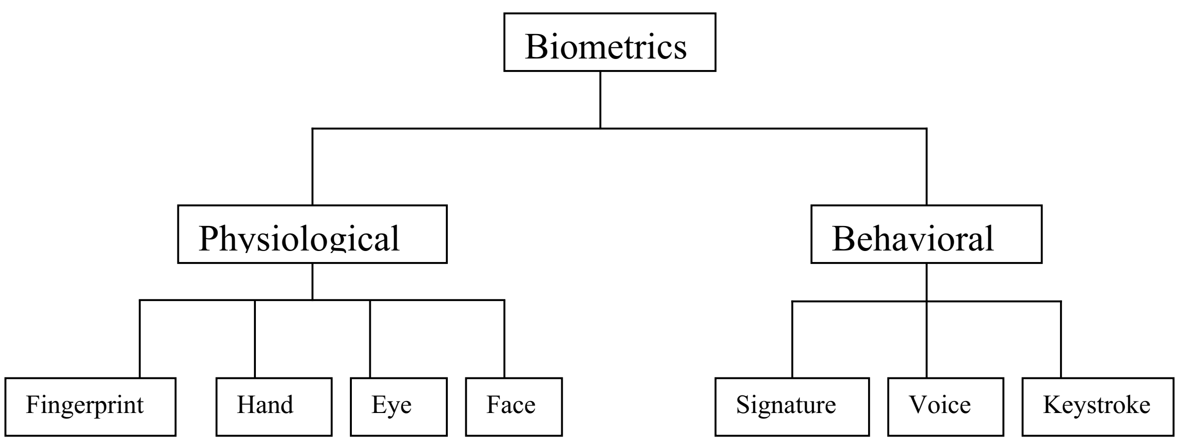
In the first part of this paper, a description of biometrics technique is given, focused on the fingerprint method. Then follows an enumeration of the problems encountered.

2.3.1 Biometric Characteristics

To be used in the process of a biometric verification, a physiological or behavioral feature must follow these requirements:

- Uniqueness
- Invariance to time
- Measurability
- Universality

In biometrics both the physical or behavioral characteristics of a human being can be used, as long as they respect the conditions stated above (Figure 2).



Source: Warfel & Miller, Inc.

Figure 2: Topology of Biometric Identification Methods [19]

The different steps, in the process of using biometrics as an authentication method, are in general:

- The feature's *acquisition*: take an image of the feature both at the enrollment of a new user and each time that a user wants to penetrate the system.
  At the enrollment, several images can be taken and the best one will be selected.
- The feature *representation*: how to capture the invariant and determining aspects of the image.
- The feature *storage* in a database, as a template for further comparisons.
- The *matching* process: for each connection attempt, the input image is compared to the template. The input image goes through the same transformations, mentioned above, than the template. The system, given a particular threshold, determines if the comparison is a match or not, according to different algorithms and approaches.

This chapter will particularly emphasize on the fingerprint authentication, the favorite biometric device at the moment for authentication.

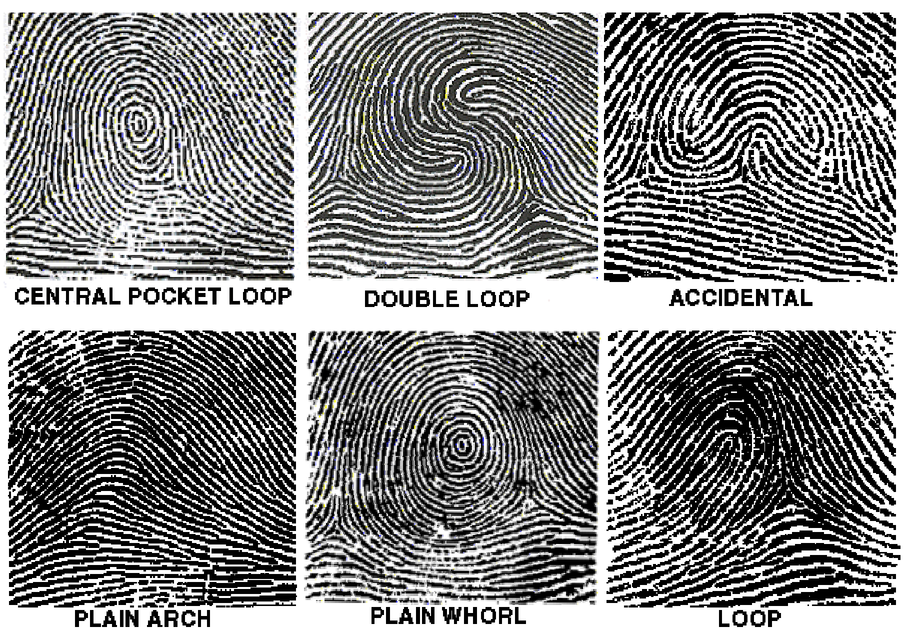
2.3.1.1 Fingerprint

Maybe the first feature thought of when talking about biometrics nowadays, is fingerprint. Even though it may still have a “bad” connotation among the public, because of its first application by the police, for criminal identification, it is one of the most reliable, affordable and simple authentication procedures. Fingerprints are formed in the embryo. They remain the same for an individual during their entire life, they can only be altered in life by accidental causes like burns, injuries, diseases etc. [20]. Nonetheless, “*Your fingerprints are formed underneath your skin in a layer called dermal papillae. As long as that layer of papillae is there, your fingerprints will always come back, even after scarring or burning*” [21]. Even though the fingerprints’ patterns are hereditary (the global features, explained in the next section) [21], they are unique. Even twins don’t have the same fingerprints. They cannot be counterfeited or transferred. Furthermore, the fingers' characteristics are different for each finger, which reduce the risks of falsification. The fingerprint authentication is a procedure known and used for a long time, especially in forensics. In the early 1960's, the Federal Bureau of Investigation (FBI) conducted studies to implement Automatic Fingerprint Identification Systems (AFIS) [22]. This has opened doors for a wider application of such systems in everyday life (access control, driver license registration, etc.).

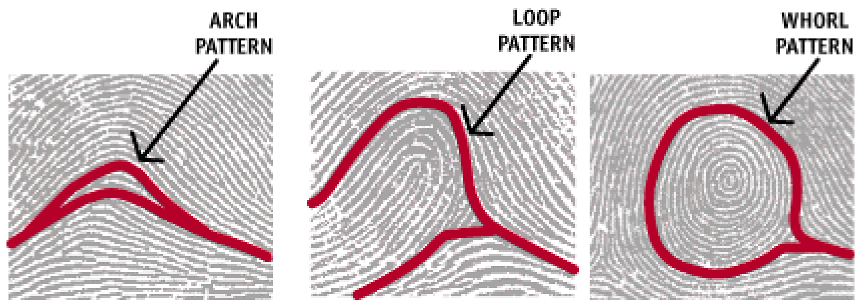
The fingerprint's structure is defined by two aspects: the global and the local features.

- **The Global Features**

The skin on the inside surface of the hands is covered with **ridges**, to allow us to hold onto objects and surfaces without slippage [23]. A fingerprint is an alternation of ridges and valleys. The ridges present "global features", visible at naked eye, that can be classified according to the FBI in seven categories [24]:



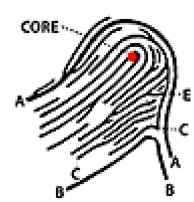
However, the most common types are [20]



This classification simplifies the search of fingerprints in databases.

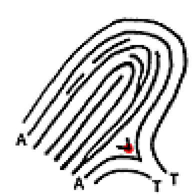
Other patterns are considered as global features. They represent singular points in the fingerprint (core, delta), ridges' characteristics (ridge count) or meaningful areas of the fingerprint (pattern area). A singular point is "*defined as a location where a local maximum in ridge curvature is detected*" [25]:

• The *Core* point is considered as the center of the fingerprint. It is the convergence point of the ridges. It helps in orienting the image.



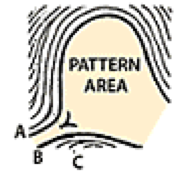
[23]

• The *Delta* point is "*the place where two lines run side-by-side and then diverge with a significant pattern area in front of the divergence*." [26]. This pattern can be a bifurcation, an ending ridge, a meeting of two ridges, a dot, etc. A triangle should be detected. The delta is a divergence point in the print.



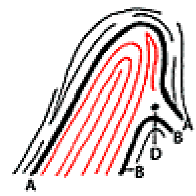
[23]

• The *Pattern Area* is the area that contains all the global features [23].



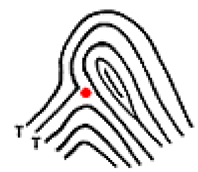
[23]

• The *Ridge Count* is the number of ridges in the Pattern Area. A virtual line is drawn from the core to the delta and all ridges that cross this line are counted [23].



[23]

• The *Type Lines* are the two parallel ridge lines that diverge to surround the Pattern Area [20].



[23]

The delta and core points are also used to indicate the fingerprint's nature for classification. For instance, the presence of only one delta testifies that the fingerprint is a loop. With more than one delta, the print is a whorl and finally, the absence of delta indicates an arch [26]. There can also be more than one core. According to the number of these two singular points, the fingerprints are organized in two different classes: the Wirbel and Lasso classes [27]. From zero to one, core and delta points, the fingerprint belongs to the Lasso group, and to the Wirbel one, otherwise. Depending on its group membership, the fingerprint's classification is more precise. The Wirbel class contains whorls and twin loops. The Lasso one contains arches, tented arches, left and right loops.

• **The Local Features: The minutia points**

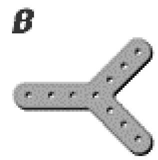
The ridges are broken, change direction, are enclosed (by other ridges) or interrupted on different locations. Those points are called **minutiae** and are referred as the "local features". **It is those minutia points details and their spatial distribution that are unique to individuals**. "… *no two people have the same types of minutiae in the same number in the same places on their fingertips*"[21]. The minutia points have been discovered by Sir Francis Galton in 1888 [22] and are sometimes referred as

"Galton's characteristics". These "*characteristics are "accidental". They are not genetic*" [28], as the fingerprint's global features.

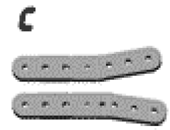
The minutia points have five different characteristics [23]:

1. *Type* (the most common are):

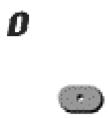
Ridge Ending



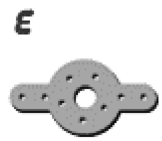
Ridge Bifurcation



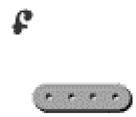
Ridge Divergence



Dot or Island



Enclosure



Short Ridge

2. *Orientation*: direction toward which, the minutia points.
3. *Spatial frequency*: distance of the ridges from the minutiae
4. *Curvature*: rate of change of ridge orientation
5. *Position*: minutia coordinates relative to specific points in the fingerprint or absolute.

Figure 3 illustrates different types of minutia points in a fingerprint image:

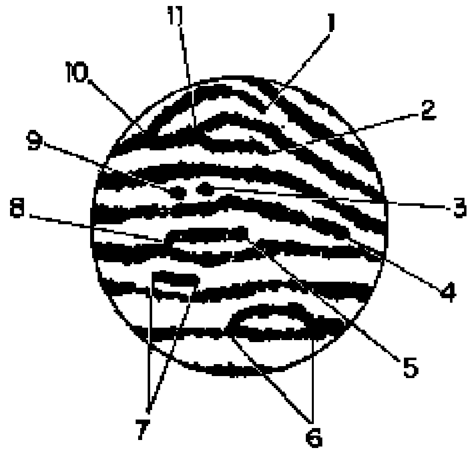


Figure 3: Minutiae Detection [29]

(1) Ridge Ending (2) Ridge Ending

(3) Dot (4) Ridge Ending

(5) Ridge Ending, (6) Enclosure,

(7) Short Ridge, (8) Bifurcation or fork,

(9) Dot, (10) Bifurcation or Fork,

(11) Bifurcation or Fork

Most of the fingerprint authentication systems are minutia-based, because of their uniqueness property. Other alternatives are a pixel-wise approach or a ridge-pattern approach, for matching, but they are less efficient for accurate identification [22]. A pixel-wise approach is based on the gray-level values of the pixels and so is too sensitive to the image quality and brightness. Moreover, it would be much longer, because it will have to compare each pixel separately and this for the whole image. The same drawback exists for the ridge-pattern procedure, where all the ridges have to be considered. Whereas in the minutia-based solution, only a few significant minutia points, among all the existing ones, are selected and matched (the ridge endings and ridge bifurcations, as explained later).

However, the main problem with the minutia-based solution is the image quality that sometimes prevents accurate localization of the minutiae or introduces non-existing ones, because of the presence of noise[4] (caused by dirt, scars, sweat, ink stains with ink-based fingerprinting, etc.). Hence, some research has been done in order to use other components of a finger image, as means of identification. The following examples are an illustration of such techniques:

– The finger crease pattern [30]

– The feature lines' attributes of the fingerprint [31].

– The finger joint line pattern on the entire image [32].

Those are landmark-based solutions. They work only on small parts of the finger, by opposition to ridge-based representations, which are based on the entire fingerprint image to detect all the minutiae. Landmark-based representations can be favored, because they offer more privacy, as the entire fingerprint image cannot be reconstructed from them [22].

In the following section, a description of a standard minutia-based system is given. It is as general as possible and does not take into account the particularities of the several algorithms implemented. Its purpose is to give a clear and simple explanation of the stages involved in this solution. As those minutia-based solutions remain the most widespread approaches.

• Description of a Standard Minutia-Based Fingerprint-Verification System

As the fingerprint representations are digital images, a few basic notions in computer imaging are presented [33]. A digital image can be portrayed as a matrix, where each element, $e(r,c)$, at row r and column c, represents the brightness value of the corresponding pixel. There are several types of images, and then several ways of coding the pixels' brightness:

- Binary Images are the simplest types of images, commonly referred to as "black and white images". Each pixel can only have two values: white or black. Thus only 1 bit is sufficient to code them, '0' or '1'. Binary images often result from the processing of gray-scale images. They are useful in

[4] Digital Scanning Glossary : « Data or unidentifiable marks picked up in the course of scanning or data transfer that do not correspond to the original."

application where the sole interest is to detect shapes or outline information in images.

- Gray-Scale Images are also white and black images, but with different levels of brightness (gray). Usually, 1 byte (8 bits) is used for the pixels' value; thus 256 different levels of gray are possible (2^8). To obtain a binary image from a gray-scale one, a threshold is used. Each pixel value below that threshold is converted in '0' (white pixel) and each value above is changed in the value '1' (black pixel).
- Color Images, also designated as red, blue and green (RGB) images, can be viewed as an arrangement of three monochromes image data. Each pixel will then be associated to three values (R, G, B), each element of the triplet, representing the level of the corresponding color. If we consider the previous model of 8 bits, here a pixel value will then carry 24 bits.
- Multispectral Images are images that contain information not perceivable by the human vision (infrared, ultraviolet, X-ray…). The information is typically mapped in RGB data.

In Fingerprint systems, only black and white images are utilized. Now, that the notions are clear, the typical automatic fingerprint authentication system can be exposed.

– *Fingerprint Acquisition*: maybe the most critical step for these systems to be able to work properly is, to ensure the best quality when acquiring the images of the fingerprints. Initially, the fingerprints' images were ink-based. The images were scanned to be stored in databases. This method has been replaced by live-scan acquisitions [22], needed with the emergence of AFIS. A faster, more efficient and more adapted solution was indeed required, to take full advantage of an automatic identification system. Efficient in the sense that the use of ink often introduced marks, leading to errors during the matching process.

In AFIS, the fingerprint is taken with live scan devices. The most popular technology is optical scanning devices where the finger is placed on a glass surface. A laser light is used to capture the mark of the ridges on the glass plateau.
Despite this improvement in the technology compared to the ink-based methods, multiple factors can affect the quality or the usefulness of the image. Those aspects will be discussed in the following paragraph. The image is then digitized.

- *Minutiae Extraction or Representation*: once the image is taken, follows the arduous task of finding the minutia points and selecting some of them to form the template. It's at this step, indeed, that the quality of the image is crucial. Here are the reasons that can cause the ridges' structures to not be well defined in an image:

– The most significant is the presence of noise, which affect the ridge configuration (by creating breaks in the ridge, bridges between ridges and overall gray-scale intensity variation [34], or holes).
– The impression conditions (sweat, dirt)
– Problems with acquisition devices
– Skin conditions (scars)

The consequences are the creation of spurious minutia points, the disappearance of real ones and the presence of errors in their localization (position and orientation) [35]. Therefore a noticeable effort is put in image enhancement, which is performed, of course, before the extraction (Figure 4). The enhancement goal is to increase the contrast between the ridges and the valleys, to remove the maximum amount of noise, without creating spurious minutiae.

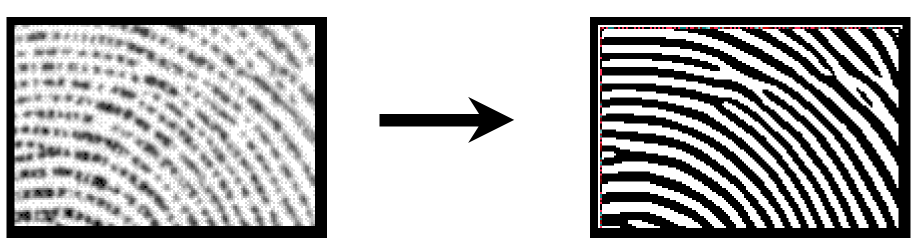


Figure 4: Image enhancement [36]

Several algorithms with different concepts have been developed for minutiae extraction. Each attempting to detect the most significant minutia points from an image, and to represent them in a way that will facilitate their comparisons.

For more manageability, most systems work only with the two most frequent types of minutiae: the ridge endings and the ridge bifurcations as firstly defined in the Federal Bureau of Investigation's model [37]. The basic minutia-based representation will select those two types and will tag them with several properties: their coordinates or position, their orientation (of the associated ridge). Prior to the minutiae extraction, an estimation of the image orientation is needed. Due to the fact that the finger may be oriented in different ways when the image is taken. This estimation is essential because it defines the ridges' coordinates.

The traditional approach follows this sequence of actions:

– Image enhancement, which can be done before or after the image binarization. As the enhancement algorithm must be modified depending on the image nature, (gray-level or binarized image) for full efficiency.

– Image binarization, to have a clear representation of the most visible ridges. Depending on a certain threshold, a ridge will be marked 1 or 0, and will correspond, respectively, to a black or white pixel, thus appearing or not in the processed image.

– Thinning (or skeletonizing) process: to reduce the ridge thickness to one pixel by eliminating the extra pixels that don't bring any original information, making the minutiae more visible.

– Extraction and Storage of the minutiae with the other related information, also called the "Encoding" phase [38].

Once the image enhancement is performed, then it is more trivial to locate precisely the minutia points, in the next stage.

- *Minutia Matching*: The matching consists in a point pattern matching. It is not an easy task, the existence of rotation, translation and scaling changes between the template and the same finger input image (Figure 5), result in differences between the minutia points. Indeed, when the fingerprint is taken at each authentication attempt, the position of the finger surely will not be the same than at the moment of the enrollment process. Not to mention the contact variations between the finger and the glass surface: some parts of the ridges may not be in complete contact with the plateau and in rare occasions, injuries can cause changes in the ridge structures [22].

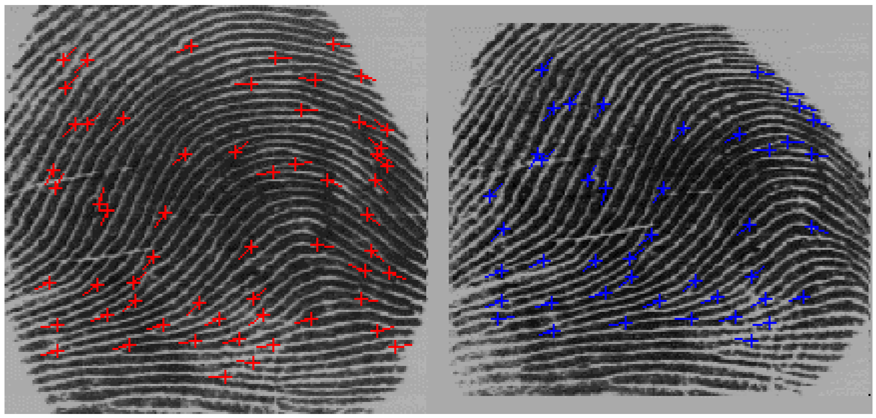


Figure 5: Matching samples of the same person [39]

The algorithms must be able to cope with those differences to be efficient.

Several approaches exist [22]:

- The energy minimization approach: "*defines an energy function based on an initial set of possible correspondences*".
- The tree-pruning approach searches over a tree for the possible matching points, by applying pruning methods, with input requirements to reduce the research space.
- The alignment-based matching algorithm: on the first step, translation, rotation, scaling modifications are performed to align the input with the template. Then the two sets of minutiae are converted to polygons to facilitate the matching process.

The major drawback of most of those methods is their execution time, which is very long, especially in the identification mode, where the input image has to be compared to a whole database (time reduced by fingerprint classification). By opposition to the verification mode where the image is just compared once to a specific template to check if the user is who she/he claims to be.

The final outcome of the systems is a Boolean value, indicating whether the checking is a match or not. This decision is based upon the definition of a **threshold** value. The result of the algorithm must be above (or equal to) this threshold for the input to be considered the same as the template.

This paper will focus on the definition of these thresholds and will try to answer several questions: How are they chosen? Can they be adapted depending on various criteria? Which criteria? How? Which improvement will it bring to a system, to have adaptable thresholds?

Of course, in this kind of systems, where a decision must be made, the error factor must be taken into account. There are two types of errors: the False Acceptance error (measured by the False Acceptance Rate) and the False Rejection error (with the False Rejection Rate). A false acceptance occurs when the system authorizes the entrance of an impostor to the system. A false rejection, when a genuine user is being refused the system entrance.

A trustable and accurate AFIS should have the lowest rates possible for these two errors. These two values vary conversely one from another:

- If the threshold is chosen in a “strict manner”, then it decreases the FAR while increasing the FRR: it will banish the impostors but will make it harder for an authorized user to satisfy the criterion.
- On the other hand, if the threshold is really “flexible”, then it multiplies the chances for impostors to be accepted as genuine users.

In the ideal case, the threshold should be chosen in such a way, that the FAR would be null and the FRR as low as possible [38].

Beside these two performance measures, others exist like the Receiver Operating Curve (ROC) which gives an estimation of the system performance at different operating points [22]. However, the FAR and FRR remain the most common measures used.

These stages represent the general procedure in a standard minutia-based authentication system.

Although fingerprint-based authentication systems represent the maturest biometric technology, in its usage at least, the other biometric characteristics also offer serious possibilities for automatic identification. Indeed, some of them are even proven to be more infallible than fingerprints.

2.3.1.2 Other Biometrics Authentication Features

Table 1 compares the different biometrics devices in terms of a certain number of requirements:

1. *Universality*: every person should have the characteristic
2. *Uniqueness*: two persons can't have the same characteristic
3. *Permanence*: the characteristic should be permanent
4. *Collectability*: the characteristic can be measured quantitatively
5. *Performance*: identification accuracy
6. *Acceptability*: how does the public perceive it?
7. *Circumvention*: difficulty degree to fool the system by fraudulent activities.

Biometrics	Univers.	Unique.	Perm.	Collect.	Perform.	Accept.	Circum.
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
Facial Thermograms	High	High	Low	High	Medium	High	High

Table 1: Comparison of Biometric Technologies [22]

"*The central issue in pattern recognition is the relation between within-class variability and between-class variability*" [40]. The within-class variations are the changes noticeable in representations of the same characteristic. The between-class variability deals with the differences between distinct characteristics (not from the same persons). Hence, the pattern used for authentication should present a small within-class variability, but a large between-class variability for efficient identification. This is defined by the number of degrees-of-freedom (distinct forms of the pattern, among individuals) provided by the pattern.

Hand Pattern

Identification can be made based on the hand shape: its size, length, width, fingers length. "*From the time you're born until you die, your hands change and yet they remain characteristically yours. The comparative dimensions. The shape of your fingers. The exact position of the joints. Myriad complex blueprints create the hand's uniqueness. That's hand geometry and the reason why an image of one's hand is the most foolproof way to guarantee identification*" [41]. Or it can be based on the blood vessels pattern, located on the back of the hand.

These traits haven't been proved to be unique for each individual and consequently, further research must be done before they should be considered as a reliable medium of authentication.

Eye Pattern

The retina and the iris are the two eye patterns used in biometrics. The blood-vessel pattern on the retina is known to be unique to individuals and hence is suitable for secure authentication. Its major drawback is that it necessitates non-negligible material investment. To be able to capture this eye pattern, a special device is placed close to the eye, which projects a light right into it. The iris also presents a unique pattern (the tissue's texture), but more accessible than the retina, as it is "directly" visible from a certain distance with a camera. The iris represents a rich pattern for authentication as it "*reveals about 266 independent degrees-of-freedom of textural variation across individuals*" [40]. Moreover, those two internal features are protected from environmental effects, unlike more exposed characteristics, like the fingerprints.

However these two features are not well perceived by the public, because of the sensitiveness and the “privacy” of the characteristics. Nevertheless their singleness property raises them among the highest (with fingerprint and facial thermograms) trustable traits for authentication.

Face and Facial Thermogram

Facial recognition is the basis of identification in our everyday lives. It is assumed that it is easy to verify people’s identities by simply viewing their faces, as a person's face is singular. When it comes to an automated system with the same goal, the task is not as easy as in the “manual” way. This system should be able to grant access to users by comparing their pictures with the corresponding templates. To prevent frauds, the criterions selected are details like the faces’ shapes, the eyes’ shapes, the noses’ shapes, etc. [42]. Still, the within-class and the between-class variabilities, tend to present inverted rates. The example of perfect twins’ faces illustrates the weakness of the pattern (it decreases the between-face variability). When aging and environmental influences increase the within-class variability [40]. As a result, the face authentication based on images can’t be considered as trustable, as biometric characteristics like fingerprints or eye’s patterns.

Another way of representing a human face for authentication, beside two or three-dimensional images, is the facial thermogram. A facial thermogram is obtained by capturing the facial heat emission patterns with an infrared camera. These patterns are the result of the passage of heat through the facial tissues, and are produced by the underlying vascular system of the face. The thermograms are processed (read and matched) by computer and may be digitized before being stored. In this case, the matching is done using mathematical algorithms [43]. Facial thermograms are more constant and reliable than faces’ images, as it relies on the vascular signature underneath the skin, rather than the external appearance.

Signature

The signature is a behavioral characteristic. Unlike the previous, it cannot be used as a reliable mean of authentication, as it can change and be imitated by impostors.

Nonetheless, the fact that it's a widely used method for people identification, especially in the financial sector, motivates the research done in this area. Several electronic devices, working with wired pens or pen and tablet sets exist [19].

Voice Print

Like the signature characteristic, the voice print is a behavioral feature. A voice changes depending on the circumstances in which the speaker is. Therefore, it cannot be verified by comparing the way words are pronounced or sound. Rather, the matching process focuses more on the characteristics of the speech.

These two last patterns are not faithful enough to provide an accurate identification. The advantage is that they are non-intrusive, well-accepted methods that would gain to be well exploited.

Fingerprint ranks first among all those devices, because it combines reliability, affordability, simplicity and wide recognition.

2.3.2. Problems encountered in Biometrics

There are four main categories concerning the problems raised by the use of biometrics [19].

2.3.2.1 Physical Security

Like any other authentication system, the biometric device itself must be safeguarded to prevent frauds. A sophisticated biometric system is needless if impostors can compromise the device, for instance by circumventing it to enter a secure place. The device must also be protected to prohibit its replacement with a tampered one. In such a case, attackers will be able to capture all valid fingerprints and reuse them later.

Furthermore, if a communication network exists between the computer attached to the device and the database storing the templates, this network should be made resistant to eavesdropping. Attackers could replace templates retrieved from the central computer for comparisons, with their own, which will grant them the system admittance. Certain existing AFIS scanners encrypt the data transmitted over the wire linking the device to the host PC [44]. This is the case for Digital Persona *U are U* [45] system and Sony *Fingerprint Identification Unit* (FIU) [46].

Another concern is about the possibility to replicate the image of a genuine user. One could imagine an impostor, replicating the marks of a print, left by a previous user on the device. These traces of fingerprints are called latent fingerprints and can be easily lifted with adhesive tape for instance [56]. There are the ones collected by the police on crime scenes for further identification. Or as illustrated in science fiction movies ("Demolition Man"), the feature used for authentication (an eyeball) can be physically removed from an authorized user to be scanned by an impostor. Fortunately, many biometric devices are able to make the distinction between living tissues and dead ones.

These extreme examples depict this threat of possible replication that biometric systems have to face. Therefore, a biometric system shouldn't be used as the single authentication system. This is not only valid for biometric methods, but for any authentication technique, to reinforce their efficiency. It is possible to associate one or more of the three authentication methods: password, smartcards and biometrics (Figure 6). Their uses are given in Table 2.

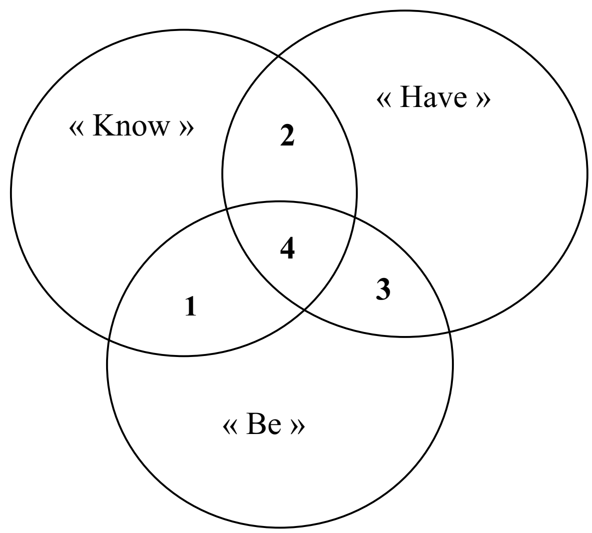


Figure 6: Model of Authentication Methods (adapted from [19])

	Authentication Methods	**Applications**
1	Passwords and Biometrics	Verification: The user enters a PIN and the corresponding template in the database is compared with the input.
2	Passwords and Smartcards	To prevent smartcards' steals.
3	Biometrics and Smartcards	The characteristic is stored in the smartcard. Example: fingerprint pattern registered on the chip, encrypted [47]. The users' characteristics are then compared with the templates stored in their smartcards.
4	Biometrics, Passwords and Smartcards	To increase the security of the option 3 above.

Table 2: Authentication methods combinations

2.3.2.2 Human Issues

A significant problem involved with biometrics is the public acceptance of this kind of authentication. It is often considered as an intrusive way of identification. The most efficient devices for accurate authentication, like fingerprints, iris and retina, are not well welcomed by users. The first one because of its criminal “background”. It is perceived by people as degrading to have to give fingerprints, as it was first done for criminals’ registration. The eye, as mentioned above, is a too sensitive part of our body, for people to agree to have it manipulated for identification. The well-admitted methods in the view of the public, like signature and voice recognition, are behavioral characteristics and not biological ones. Therefore, they are less trustable.

The priority for biometrics’ survival and expansion is to overcome the human resistance, and make people feel more confident in using such solutions. In everyday life, it is not yet perceived as “normal”, to have a fingerprint, or iris pattern taken. For now, it is applied most exclusively in high security areas. Users surely need more time to evolve and stop being suspicious about these techniques.

Another important criterion for the public is the execution time for authenticating a user. This is a drawback of biometrics, which is much slower than other authentication methods, like passwords or smartcards authentication. Due to the time required to process a feature’s input and to compare it with the template. Particularly, in the identification mode with a substantial database. The input will have to be compared to the whole database in order to find a match or not, as the user is completely unknown. In the verification mode, an improvement is brought, because, the user first chooses a template by submitting a PIN for example. The system then confirms whether or not the user is the “owner” of the template, by comparing the input only with this image retrieved from the database. Emphasis should be put on the speed of the matching process; otherwise this disadvantage will hurt biometrics’ approval.

2.3.2.3 False Acceptance and False-Rejection Rates

Unlike the other methods, biometrics involves a margin of error in the authentication. As the features compared cannot be recognized “all-or-nothing”, like passwords or smartcards. “*The data do not follow a fixed profile but are altered by non-negligible intra-individual variations, but which are largely inferior to inter-individual variations*.” [47]. Clearly, at the enrollment and at the authentication phases, the same pattern, can be slightly different, depending on the conditions in which it has been captured. Thus, making the matching process not as trivial as for the other authentication techniques. Hence, the apparition of these two error rates: the FAR and FRR, non-existent elsewhere. A certified user does not want to be rejected by the system, and so finds less disturbing to have a FAR greater than the FRR. Some systems allow the tuning of the acceptance or rejection criteria [44], others don’t. For instance, the ABC *Biomouse* product [48], offers as an option, the configuration of the FAR, between 1/500 to 1/1000000. This property has to be manipulated with caution, to avoid weakening the system. Those two rates are completely dependent on the threshold chosen. In an adaptable threshold system, they will vary, according to the criteria used to modify this threshold. However, they should always be kept as low as possible.

2.3.2.4 Cost

The implementation of biometric authentication is expensive because of the reader’s complexity [47].

2.3.2.5 Degradation of the Biometric Characteristics

“*Will the system detect the slow, purposeful incremental erosion of the biometric trait?*” [49]. This question raises an interesting issue: the gradual “deterioration” of most of the biometrics characteristics, which happens with time, climatic conditions or diseases. A biometric authentication system should address this nonreversible phenomenon, to extend its own longevity. The Sony FIU [46] has solved the problem by offering a special software configuration to the users: " *the adaptive verification*". This mode progressively replaces old data enrollment by more recent fingerprints. This solution is appropriate only if the system is completely efficient and correct for authentication, with a FAR equal to zero. Indeed, if the enrollment data are replaced by input fingerprints that have passed the test, then those inputs should be exempt from any doubt or error.

After presenting the concept of biometrics, the next section looks at the application of this authentication technique to electronic commerce and the world of cellular communications, as expected in the middle or long run.

2.3.3 Adapting Biometrics to Electronic Commerce and Cellular Telephony

The efficiency offered by biometrics based authentication systems, could be used to secure electronic commerce and mobile telephony. In the two next paragraphs, an AFIS employed for a commercial site is pictured, as well as a procedure to protect a cellular phone.

2.3.3.1 Electronic Commerce

The introduction of biometrics in the field of electronic commerce will make it far more secure than it is currently, but at the expense of a dramatic rise in the costs for the customers. Indeed, it involves that all clients, who want to do online commerce from home, should possess an authentication device connected to their PCs. They would use these devices to capture their characteristics and send them (encrypted) via the network to merchants. Public-key encryption can be a solution for customers and merchants to communicate securely over the network. They both would exchange their public keys and use them to encrypt the data they're sending. Digital signatures also may be useful, for data integrity, however if authentication information are stolen over the network, they won't be altered, as the impostor wants to impersonate the user. To avoid replay of encrypted characteristics, a solution would be to number the stream of data (user's characteristics) when it is sent for authentication. Both the user's device at home and the merchant one will keep the last transaction number for each client. If both numbers don't match, it will mean that the information was sent from somewhere else than the user's PC and the authorization will be denied until the user is notified. Due to the encrypted nature of the information, even if it is intercepted on the network, the impostor will have no way of knowing the transaction number. As the customers' characteristics are biometric and are not saved on their machines, it is sure that, at home, they provide from the correct person. Upon receipt of the information, the merchants would then compare the inputs with the templates obtained at clients' registrations, for identification. An additional precaution would be to impose the physical presence of the clients for their enrollment (for increased security on the client's identity). On the other hand this procedure would restrict the merchants' potential clients circles, to their own cities. Making them lose the major benefit of electronic commerce: the "interplanetary village" notion brought by the Internet.

A futuristic idea would be to imagine merchants' sites that will allow the clients to scan their fingers (for AFIS) directly from the PC screen at home. A special tactile window can be pictured, on the merchant web site, visible on a corner of the client's screen that will represent a miniature scanner. This solution of course resembles more a "sci-fi" scenario than a realizable method. Still, the logic is to transfer the device from the clients' homes to the merchants' sites, to suppress the investments needed by the customers and make the biometrics authentication more attractive to them. A higher authority, based on the model of the Certificate Authority, would be preferable, to provide control over the system and issue authorizations to merchants, wanting to capture customers biometric characteristics on their websites. This authority could then keep track of the merchants and rule the use of the customers' information. Before dealing with a merchant, the customer would first check its authorization with the authority.

Whatever may be the technical achievements required for the setting up of this technology, biometrics represents the next step in securing electronic commerce, as it simply represents the next generation in authentication procedures, in all areas.

2.3.3.2 Cellular Telephony

"With the FingerChip™ integrated into a cellular phone, a user can be verified by comparing a live fingerprint against the one or few stored in the phone's memory. And should you need to lend your phone to family or friends, the FingerChip™ could be engineered so that additional users could be added at your convenience by placing your fingerprint on the sensor, authorizing the addition of new users." [50]. This fingerprint chip, developed by Thomson-CSF presents a way of implementing biometrics for cellular phone security.

The use of voice verification, like the Authentix RVR technology, is also a biometric authentication, applied to cellular phones. However, as the voice pattern is not reliable enough for a certain authentication, it shouldn't be employed as the unique security device.

These two characteristics: fingerprint and voice are, in my opinion, the only exploitable biometrics traits for cellular phone authentication, due to the shape of a cellular phone and the way it is utilized.

Summary and Transition

Biometrics authentication is the oldest authentication method used, but still has a bright future because all the opportunities haven't been exploited yet. As the need for authentication becomes stronger, the most efficient devices are required, which can be offered by biometrics.

One of them, the fingerprint authentication, meets at the moment with universal approval, among biometric devices.

The primordial problem biometrics has to overcome is the human issue, which is a determining aspect in the success of a technology.

After presenting the three existing approaches for authentication (knowledge, possession, and biometrics), with an emphasis on fingerprint authentication, the next chapter now focuses on the parameters used in a fingerprint-based authentication system. These parameters are the acceptance thresholds, the FAR and the FRR. An analysis of the adaptability of these parameters, for a better flexibility of an AFIS, is given.

Chapter 3: Possible Criteria for Threshold's Adaptability

Most of the fingerprint identification systems use fixed acceptance thresholds for authentication. The threshold depends on the algorithm selected for the system. The algorithm will determine, according to the matching technique employed, the acceptable value that should be assigned to the threshold. The selection of the threshold has also repercussions on the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). If it is strict (high value required for the matching score), as strong authentication is required, the risks to accept an impostor are low (the False Acceptance Rate decreases), but the improper rejection of a genuine user is more likely to happen (the False Rejection Rate increases). On the other hand, if the threshold is chosen in a "lax" way, the effects on the acceptance and rejection rates are inverted.

In general, there is one threshold set for each system, regardless of the external conditions of the testing, the inner characteristics of the fingerprints or the application's nature. This can introduce high error rates, either acceptance or rejection type, because of the application non-flexibility. In an effort to narrow the False Rejection Rate, the goal of "adaptable parameters" is to make the authentication system as flexible as possible, without weakening it (by maintaining the FAR as low as possible). The previous section suggested that a key condition to biometrics success was its wide acceptance by the public. Indeed, a system with a high FRR is particularly inconvenient for the users. If, instead of coercing the users in enduring such a drawback, the system's parameters could be adapted to the users or the other elements, then it would dramatically improve the authentication results. This is feasible by taking into consideration all or some of the conditions described above. The following chapter will mainly discuss the possibilities of decreasing the threshold, to make the system less constraining for the users. Except for one situation where the threshold will need to be increased for security questions.

The issue here is to know whether and how those different criteria can lead to the modification of parameters like acceptance thresholds in authentication systems.

The adaptability of the FAR and FRR will not be considered, because these two parameters are completely connected to the threshold. The only way to affect these variables is by varying the threshold. Hence, the chapter will only focus on the threshold modification, which causes both rates' correction (conversely one from the other as previously explained).

Three classes of criteria can lead to threshold's changes:

- The fingerprints' characteristics, namely the minutiae.
- The authentication system's nature.
- The environmental and external conditions.

However, correlations exist between some of the criteria in their effects, either on the fingerprints, or on the system as a whole. For instance, the geographic distribution or density of the minutiae, as well as the environmental or external conditions during the scanning, can result in a lack of exploitable minutiae in the images. These are three different criteria, that raise the same problem and thus the solution chosen will certainly be similar, for the three of them.

The threshold's value is not significant "on its own". It is meaningful only when related to the algorithm it relies on. It is computed in such a way that, it takes into consideration the number of minimum minutia points required for a correct matching, as well as other parameters specific to the algorithm.

In the algorithm for fingerprint identification designed by X. Qinghan and B. Zhaoqi [51], as an illustration, the pattern used is the feature line of a minutia point, the line joining the core point to the minutia. The matching consists in comparing each feature line of the input image to all feature lines of the template, within each quadrant. The closest feature line in the template, regarding the feature lines' attributes, is selected. The matching score is computed according to the dissimilarities between the feature lines' attributes of the input and those of the selected feature lines in the template. The matching score increases when the dissimilarities decrease. The minimum number of matched minutiae required doesn't appear clearly, however it represents an necessary datum in all Automatic Fingerprint Authentication Systems (AFIS).

Concerning the value of this minimum number of identical minutia points for a match, between a template and an input fingerprint, the FBI Manual of Fingerprinting states that twelve matched points is enough for a positive identification. Nonetheless, in the absence of a defined rule, eight or more is accepted as a standard [52]. In the following discussions, twelve will be the value used as a standard.

3.1 Fingerprint Features

The first category of criteria concerns the minutia points. Depending on their geographic distribution, density or type, they may or may not be relevant for the threshold's modification.

3.1.1 Geographic distribution of the minutiae

The minutia points are unevenly distributed on the entire fingerprint. The minutiae's locations vary from one individual to another. As these particular points are accidental, they permit the accurate identification of an individual, thanks to their uniqueness. The geographic distribution of the minutiae refers to the general localization of those special points on the fingerprint (centralized, left-oriented, etc.). Does it affect the threshold to notice that for some people, the minutiae are more concentrated on the left of the image, or for others on the center? And is it even rational to assume that minutia can be more concentrated on a particular area of the fingerprint? Surely there will have some cases where no particular "minutiae grouping" will be detectable and others where a slight concentration will be noticeable. The idea here is to imagine the situation where, because of the geographic location of the minutiae, the algorithm cannot collect sufficient minutia points to perform an accurate matching. Due to the fact that it doesn't process the appropriate area. Consequently it can be assumed that the threshold's value is not adequate in this situation, because there isn't enough data to correctly execute the algorithm. A solution that one could advocate, would be the threshold's modification according to the geographic disposition of the minutiae.

An extreme example can be considered, where a particular input fingerprint **does not present** on the examined area, the required twelve exploitable minutiae points (because most of the points are located on a different region). This scenario will be treated until the end, even if it isn't realistic, only to find out if the geographic location of the minutiae can constitute a criterion for threshold's adaptation. One of the assumptions is that the algorithm works only within the window shown in Figure 7. The algorithm will pursue based on the points it can collect.

1. Even if the input is compared with the **same finger's template**, the matching score will not reach the threshold, as the number of minutiae is lower than the standard, even if all points match. The template (processed with the same algorithm) may show the same number of identification points than the input, but this is not trivial, because of the orientation and position changes when the fingerprints are taken, not to mention the image's quality that can dismiss genuine minutiae. Hence, the input's window may not show exactly the same area than the template's one (Figure 7).

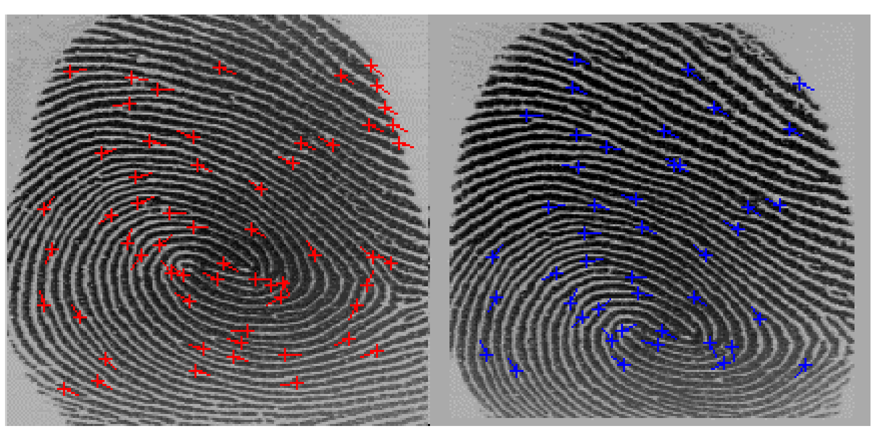


Figure 7: Before orientation estimation [53]

This is where image orientation estimation is useful to define invariant coordinates for the ridges and the furrows [54]. A singular point can be chosen as the reference point of the coordinates system (Figure 8), like the core point in this picture. In the absence of singular points (in arch type fingerprint), the center of the global feature itself (arch, loop, whorl, etc.) can be chosen as the reference point.

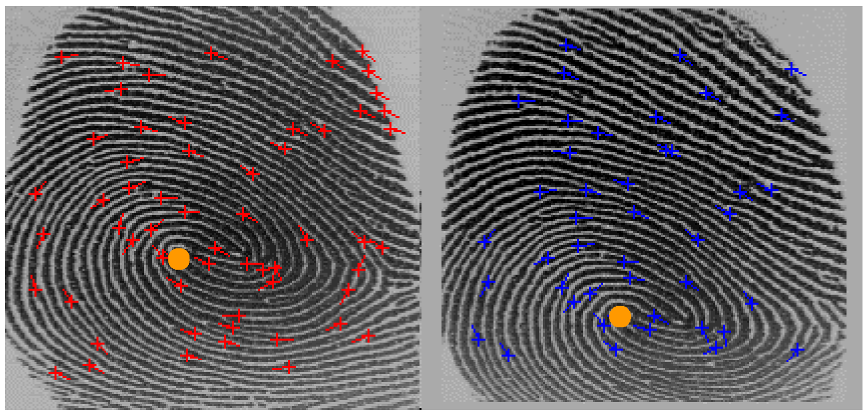


Figure 8: After orientation estimation

In this example, after the manual orientation process, according to the core chosen as the reference point, both windows present approximately the same region. However, whatever is the image that has the maximum number of minutiae, only the lowest number counts (inferior to twelve, the standard for a trustable authentication).

2. When the input is equated with **another person finger's template**, (Figure 9) two general cases are imaginable :

   – Due to the distribution of the minutiae on the whole fingerprint, the algorithm detects enough minutia points on the template. Then here also, after the definition of the image orientation, the lowest number of minutiae will be the maximum number of matched points. Which is the input's number of minutiae (according to the initial assumption, less than twelve). Furthermore, it is unlikely that the number of matched points even equals this minimum number, because it is not the same finger. In any cases, the matching score will not reach the threshold.

– The template also displays a concentration outside the window that prevents a sufficient amount of points to be present within the window. Same consequence as above, the score is not sufficient for a positive authentication.

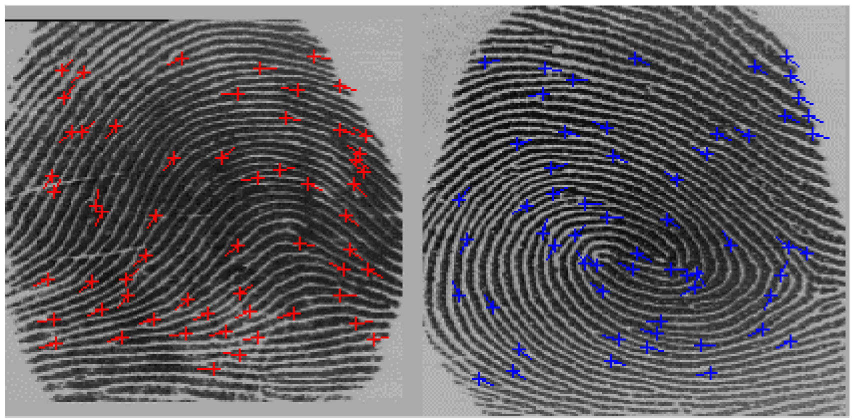


Figure 9: An arch compared to a loop [53]

In all these cases, the threshold is too high and a genuine user will be rejected. Due to the absence of minutia points for a correct identification.

In the case of adaptable thresholds, there should be one different threshold for each possible situation, previously identified and defined. However, it is absurd to define one threshold for a left-oriented location, one for a right-oriented location, one for a centered location, because the threshold for the left-oriented location, will not differ from the one for the right-oriented location for instance. Moreover, the algorithm will not process the right or left region, where the minutiae are, but the one within the window. Therefore, it is more appropriate to set one threshold for the images where most of the minutiae are within the window, and another one when minutiae are outside the window. Before doing so, the circumstances where this particular threshold can be applied should be determined. A difference should be made between the situation where not enough minutiae are collected because of their geographic distribution and the situation where the minutiae have been eliminated due to the image poor quality. If the algorithm just changes the threshold each time it does not extract enough minutiae from the prints, then the authentication system will be insecure in its conception. To allow this differentiation, a special classification stage could be performed just prior the matching process, to estimate the global minutiae's position. If, within the window a lack of points is estimated and a particular concentration of minutia points is detected outside this window, then the adapted threshold can be applied. Otherwise, if the first condition is respected, but not the second, meaning that more points cannot be found outside, then there is no reason to change the threshold.

One could argue that the "image poor quality case" is exactly identical to the first, and that the threshold should also be modified in such a situation. Indeed when minutiae disappeared because of an image's poor quality, then the system could be made a little more flexible to avoid a high FRR. This point will be discussed later in the paper.

Nevertheless, even if each case is identified before applying the adapted decreased threshold, the identification system remains breakable and can't be reliable. As the result is the same even if the initial conditions are distinct. If the threshold is lowered, it weakens the system, by increasing the FAR, because the constraint is simply released without bringing any compensation to this measure.

The solution resides in the **modification of the algorithm, not the threshold itself.** It will be more optimal to only move the "processing window" toward the area exhibiting the maximum minutiae, and to leave the rest of the algorithm unchanged, instead of having a different threshold for each specific location. Furthermore, it increases the degree of correctness in the matching process thanks to the presence of more identification points. The special classification stage or "distribution " stage must remain to provide the coordinates for the new window's position.

The core point can be used to define the image's center (when applicable), to make sure that the finger was correctly positioned on the glass (some users may show the side of the finger instead of its face) [55].

The scenario chosen wasn't really realistic because it implies that algorithms work only on really restricted areas of the prints, whereas in the reality, the image is large enough to consider the whole pattern area. And even, under such circumstances, the number of identification points in a fingerprint is so high (100 or more [52]) that a “representative” portion of it, is sufficient to extract a satisfactory number of points. “Representative” in the sense that special areas of the print (area around the delta, for instance) are more likely to be surrounded by more points than others (area near the finger’s tip) [52]. The size of the fingerprint image is of course crucial, but usually it is large enough to find a correct number of points.

To conclude, this criterion of geographic location of the minutiae is not valid for threshold’s adaptability, because it cannot guarantee a correct level of reliability.

3.1.2 Minutiae’s density

The minutiae’s density problem raises the question of the template’s size. The assumption is that some images may present a higher density of points within a smaller region, than others, for which the system will have to consider a larger area. How the threshold is affected in such a case, if it is only a matter of size? The issue here is the same as the one of the minutiae’s geographic location, treated above. It comes from the fact that the system can’t detect a sufficient amount of points in the image presented.

The previous paragraph explains that in case of insufficient points collected, the solution resides in the modification of the extraction stage, instead of the threshold. Whether the lack of minutia derives from a geographic concentration of minutiae on another area of the print, or is due to a low points’ density in the fingerprint, it mustn’t alter the threshold. The minutiae’s density, like the previous criterion, doesn’t affect directly the threshold. In the previous case, the solution was to move the “window” to the region exhibiting a minutiae concentration. Here, the solution resides in the enlargement of the image.

As an example to confirm this assertion, an input is compared with a template with a higher density. Then the template will present more points on a smaller region. On the other hand, the input’s processing area will be larger, to be able to reach the same number. One could think that if the two images were extracted from the same finger, then they would show the same density. The density is the average number of minutiae per space unit, it doesn’t mean that the number of points is the same from a location to another. This can possibly happen if the algorithm succeed in correctly orienting and positioning the input image, according to the template in order to examine the same regions. If the images don't have the same origin or can't be correctly re-oriented, then the extraction stage's algorithm will present the following logic:

*"**WHILE** [(not enough minutiae detected for one of the images)* AND *(limits not reached)] **DO** (extend both images)"*.

Both images will have to be enlarged, otherwise, the minutiae will be collected from different parts of the finger and the matching will not have any chance to succeed, even with prints of the same finger. If some images at their maximum size still don't present enough minutiae, then this may be due to external reasons (noise, injuries, etc.). This case will be considered later on.

Affecting the threshold may solve the problem but at the expense of a security gap.

Nonetheless, most of the authentication systems don't operate this way. They don't start working on a restricted area to enlarge it after, when required. They rather consider the entire fingerprint and search for minutiae on the whole image. So, in this case, as the image can't be enlarged anymore, lessening the threshold may appear as the unique solution, but only if the new number of identical points, corresponding to the new threshold is greater than the minimum demanded (twelve). Yet, this solution is illogical, because the threshold is a value representing the minimum acceptable result. Thus, it certainly already corresponds to the minimum identical points demanded. Lowering it will once again weaken the system.

3.1.3 Minutiae's Type

As mentioned in the first chapter, the minutia points have different shapes or types. The most commonly named are listed in Table 3:

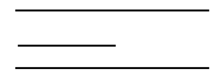
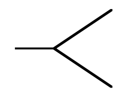
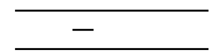
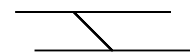
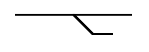
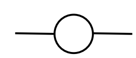
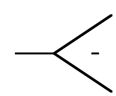
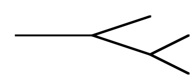
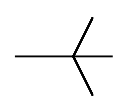
– Ridge ending	
– Ridge bifurcation	
– Island [5] or Short ridge	
– Dot [6]	
– Bridge	
– Spur or Hook	
– Eye or Enclosure or Island [5]	
– Delta	
– Double Bifurcation	
– Trifurcation	

Table 3: Common Minutia Types [28]

Some of them are more frequent than other. This is the case for ridge endings and ridge bifurcations for example, compared to trifurcations that are among the rarest features, not to say are the rarest type. Based on this knowledge, the fact that the various minutiae's types have different probabilities to be found in a fingerprint,

5 Depending on the sources of documentation, an Island type minutia may be equivalent to a Dot type or, in other documents to an Enclosure type.

here again the threshold's modification according to the type detected, can be conceived.

In the method defined by J. Osterburg, T. Parthasarathy, T. Raghavav and S. Sclove [28], assigning "*a probability to a fingerprint ... based on the number of individual (Galton) characteristics present*", a study is conducted on a set of 39 fingerprints. A grid of one-millimeter squares is placed over each fingerprint to partition it into cells (for a total of 8,591 cells for the 39 images). Each cell can be either empty or can contain one or several minutiae. The method considers ten Galton characteristics [7] (bridge, dot, ending ridge, bifurcation, island, lake, delta, spur, trifurcation, and double bifurcation) as well as groupings of multiple characteristics in the same cell. The empty cells are also considered as a kind of particular minutia's type, but are not relevant for the present discussion. The repartitions of these minutiae types in the cells are analyzed. The occurrence probability for each pattern is then computed and global probabilities for given configurations are estimated. The real interest of this method in the present concern, is that it provides information on the minutiae's types frequencies. The grading of the different patterns' occurrence probabilities is shown in Table 4 (only occurrences of single type within one cell are represented, and the empty cells, the most frequent, 77%, are not mentioned either):

6 A Dot is a ridge that is so short that it appears as a dot.
7 The dot and the island minutia types have different shapes in the article of Osterburg, Parthasarathy, Raghavav and Sclove.

Grade	**Minutia type**	**Estimated Occurrence probability (p_i) [28]**
1st	Ridge ending	0.0832
2nd	Ridge bifurcation	0.0382
3rd	Island	0.0177
4th	Dot	0.0151
5th	Bridge	0.0122
6th	Spur	0.00745
7th	Lake	0.00640
8th	Delta	0.00198
9th	Double bifurcation	0.00140
10th	Trifurcation	0.000582

Table 4: Grading of Minutia Types Occurrences

Yet, the majority of the cells (77%) were empty. However, the table gives an idea of the distribution and will be used in the remainder of the section as a reference for the type's rarity.

The idea is to prioritize the matching of scarce points, by diminishing the threshold in terms of number of matched points required for a positive authentication. If certain points are more infrequent than others, then when one of them is noticed, it is more optimal to focus on this point for the authentication, as it is really improbable that a different person's fingerprint shows the same point at the same location. Thus, lessening the threshold can be interpreted as matching fewer but more meaningful (because uncommon) points in the prints. Moreover, it speeds up the process.

Still, the simple localization of a rare minutia's type is not a sufficient condition to decrease the threshold. It will make the system unreliable if the threshold is systematically lowered before knowing if the rare minutia will match in both fingerprints. The algorithm here can be stated as "as soon as the same singular minutia is found in both images, (at **approximately** the same location), then fewer points are required to confirm a positive identification". This rule's validity increases with the minutia's type rarity. The presence of additional points for confirmation is essential, because even if the singular points are rare, they are not unique. Hence a conclusion based on a single match is not reasonable, whatever this match is. It should also be pointed out that when a rare type is detected in only one of the images, (instead of both the input and the template), it does not automatically mean that the fingerprints don't come from the same person. Several different reasons, like the image quality, or injuries on the fingers, can cause the disappearance of genuine minutiae. In this case, the comparison with the other minutiae will be decisive for the conclusion. Consequently, as single patterns are not sufficient for authentication, even though they are reliable points, a better solution would be to work with clusters of points. This method prevents an increase of the FRR. Yet, the threshold's modification can take place only after the matching of the particular point. However, in general in AFIS, the algorithms don't pay attention to the nature of the minutiae that have matched but rather to their number. If this scheme of adaptable threshold has to be applied, then there should be a way of knowing whether or not the singular minutia has matched, before altering the threshold.

The threshold's value depends on the minutia type's rarity. If a very rare minutia is present on both the input and the template fingerprints, at the same location (after image orientation) then the probability that the fingerprints belong to two different persons is very low. This situation should be reflected by the threshold value. Indeed, the matching of this rare minutia as well as a *few* others, surrounding it, will be enough to conclude to an equivalency in both images. On the other hand when quite common minutiae are extracted, then an appreciable number of other points must correspond in order to confirm the authentication. The determination of these numbers of supplemental points constitutes the threshold definition.

A possible algorithm for an adaptable threshold system is described, from the minutiae extraction stage:

1. Each minutia extracted from the input fingerprint is associated with its "rarity weight" (as part of its properties). The weight can be estimated after a study on a large database of fingerprints.

2. A classification of the input minutiae, based on their weights is performed before the matching. In the descending order, from the highest weighted minutia (the scarcest) to the lowest weighted one (the most frequent).
3. Then the matching with the template is executed in the order of the grading. Assuming that the template's minutiae have also already been classified.

   Declaration of the variables used in this algorithm:

   i: Minutia in input list

   j: Minutia in template list

   Wi: Weight of the input minutia i processed

   Wj: Weight of the template minutia j processed

   Flag: Boolean

   T: Threshold value

   Nx = Number of matched points (threshold) associated with the minutia x's type.

   Here is a portion of the algorithm, concerning the minutiae's comparisons:

```
i=1; j=1; F = 0; T=100 //arbitrary value
while (T>0) and (i <= EOF_Input_List) and (j <= EOF_Template_List)
        if (Wi=Wj) then //same minutia's type
           Try to match both points;
           if (match) then
              if (Flag = off) then
                 T=Ni; //Ni is chosen according to i's weight*
                 Flag=on; //Set Flag on
              endif
              T=T-1; //the singular minutia's already matched
           endif
        endif
        Select next (i, j) to compare
end while
```

- The algorithm starts by the first minutia in both lists (input and template). Before matching two minutia points, the algorithm simply looks if their relative weights are identical. If they are not, then it is unnecessary to compare them, because it's already sure that the points are different (not the same type). Indeed, the same minutia's type will have the same corresponding weight in all images.
- If the comparison is a match, then depending on the weight value, the number (Ni) of points that have to correspond, for this particular minutia i's type is set. The rarer the first minutia is, the fewer the additional points will be. *This number Ni represents the threshold's value* (considering the threshold value as the total number of matched points: the additional points plus the singular one). The algorithm then selects the following points in both lists.
- In the case of a negative comparison (the same type but not the same point), the algorithm just picks up the following point in the template list and starts over the process, keeping the same minutia point in the input list

(i). The algorithm only moves forward in the template list, because a single type can be present more than once in a list, thus the next minutia in the template list can also be of the same type than the input minutia.

- As long as the input minutia’s weight is inferior or equal to the template’s one, there are still chances to find this input minutia’s type in the template list (due to the descending sorting of the lists). On the other hand, when the input’s weight is greater than the template’s one, the algorithm considers the following point in the input list but keeps the same template’s minutia, since there is no chance left to find the input minutia’s type in the template list (sorting on the lists).

4. The flag F is employed to prevent the threshold’s value redefinition each time a match occurs, it should be done only once, at the first equivalence found between the points. The threshold is decremented at each positive match. If there is no matching until the end of the list, then the threshold is not set and the algorithm can immediately conclude to a negative comparison.
5. The algorithm stops either when reaching the end of one of both lists, or when the threshold value reaches zero.

The image orientation is determining, because the minutia must be detected in the same region in both fingerprints.

This criterion, the minutia’s type, is the first one so far to constitute a serious candidate to threshold adaptation. Indeed, adapting the threshold to the minutia type doesn’t automatically weaken it, like in the previous cases. The threshold will be lower only when a rare type will correspond in both images, confirming the improbability for two different persons to have this same minutia at the same location.

3.2 Application nature

The characteristic of the site itself, protected by the authentication system can determine the threshold value.

3.2.1 Commercial Application

This paragraph will consider the usage of an AFIS, as a method for authenticating people for commercial purposes. The case study is an AFIS implemented for a company online for electronic commerce for example. The system will work over the Internet. This section will not deal with the threats of information interception during their transmission over open networks, data integrity and security are assumed. The question raised is still the same than the one stated in the whole section: can the threshold for AFIS be lowered (in the electronic commerce domain)? If it is decreased, then the authentication may not be accurate and it will lead to an increase of the FAR. The FAR implies that impostors will be improperly acknowledged. The system here is a commercial site. What are the consequences of false users accepted in such a case? They will buy merchandises in the name of the impersonated genuine users, who will be charged.

The electronic commerce as presented in the first chapter, is done in diverse ways, in view of both, the nature of the goods ordered, as well as the payment solutions available to the users. To be able to assert whether or not the threshold needs to be changed in this situation, an analysis of all these aspects is needed. There are two kinds of goods marketed in electronic commerce: goods as data that can be transmitted over the net (news, graphics, multimedia clips, web page access, etc.) and objects that are sent by regular mail services. Concerning the payment methods, electronic cash, credit card applications and electronic checks are the means in use. According to the merchandises ordered and the payment solution chosen, the impostor may or may not fool the merchant. This scenario supposes that the impostor has succeeded in being authenticated as a genuine user. Whether due to a non restrictive AFIS or by supplying a copy of the user's fingerprint (print left on the device). Regarding the payment methods, as the electronic cash is stored on the user's PC, it implies that the impostor must do the transaction from the genuine user's PC. With credit card applications, there are three existing procedures:

- The user may need to provide the credit card information prior to each transaction.
- The information is held by an intermediary and clients are given login names and passwords they use.
- The credit card is registered in the client's electronic wallet on the hard disk.

An electronic check constitutes a particular feature and its conception would surely differ if protected by an AFIS. As it is not at the moment a widespread payment solution for electronic commerce, it has been ignored in this section.

Payment / Goods	**Data transmissible by the network**	**Merchandises sent by mail**
Electronic Cash (virtual community)	**1**	**2**
Credit Cards (information sent each time)	**3**	**4**
Credit Cards (intermediary)	**5**	**6**
Credit Cards (in a wallet)	**7**	**8**

1. If impostors pay with electronic cash, then they do it from the users' PCs. Some software requires the user's password only for the money transfer from the account to the hard disk (*ecash* from Digicash). Consequently if there is money left on the computer, the impostors can buy anything transmissible over the net. The genuine users will be aware of the fraud only after consulting their transaction logs. Electronic goods are either sent by email or downloaded from the merchant's site after receipt of the clients' payments (*ecash* from Digicash). In this possibility, the impersonators will retrieve them from the computers' hard disks. On the other hand, if they are sent to the genuine customers' emails, then the impostors have to get over an additional obstacle: the emails' passwords.

2. If the goods have to be sent by mail, then the real users will most probably receive and return them to the merchants. Frauds using electronic cash suppose the impostors are familiar to the users, to have access to their computers and to know about the payment software. A simple thief will not take the time and risk to explore the PC content.
3. The use of fingerprint as an authentication procedure suggests that even for credit cards purchases, the clients have to be listed in the merchant's database with their corresponding fingerprints. Otherwise, the AFIS is needless. However, the credit card information transmission is still an unavoidable process, because some users don't trust intermediaries. Nonetheless, the sole knowledge of those information (numbers and expiration dates) is no longer sufficient to impersonate their holders. Indeed, two conditions are necessary for allowing frauds: first, impostors have to reproduce the users' fingerprints and moreover they should possess their credit cards' information. This scenario may happen in extreme cases, however it is very improbable. If it occurs, then the impostors obtain the data ordered and the credit cards are debited. Yet, once again it requires the impostors' presence at the users', for the fingerprint duplication and eventually the data receipt.
4. The goods will be sent at the real users' addresses. It is unlikely that the impostors succeed in intercepting them.
5. In the presence of intermediaries, it is more likely that the fingerprint authentication will replace the username and password usually submitted for identification. Then, the real owners will be charged, when they will be acknowledged (correctly or not) by the system. In this latter case,

depending on the way the data are delivered, the impostors may be able to pick them up.

6. Same result than in the fourth case.

7. This payment is equivalent to the electronic cash one. Access to the wallet is required. The fraud possibilities rely on the security protocol set by the wallet. Usually, its access should be protected by a password at least.

8. Same conclusions as in the seventh and sixth situations.

Another case, not studied above is the possibility for a genuine user to be identified as *another* genuine user, when entering the system (wrong authentication of the fingerprints). Most of the systems surely welcome recognized users by displaying their names. If the wrongly authenticated users realize the mistake, they may either, exit and retry the authentication, or take advantage of it. If it concerns the purchase of data, then the “genuine impostors” may receive them. However, it is not in their interest to try to take advantage of the situation, if the payments are done by electronic cash, as it will be taken from their own computers. Concerning credit cards (still in the context of electronic data purchases), it depends if the system includes or not intermediaries or if the cards are stored in electronic wallets. In the first prospect, the frauds will succeed because the fingerprints represent the only mean of identification and the intermediaries already possess the credit cards’ information and will use them for the payments. In the absence of intermediaries, the impostors are not supposed to know anything about the users they are impersonating, thus they will not be able to provide the credit cards numbers and expiration dates. Finally, in the last situation, the impostors again cannot obtain the payment information. With the other type of purchases, as they will be shipped to the real users’ addresses, the case is not pertinent.

To conclude, the threshold associated to commercial sites AFIS should be manipulated with caution. In the presence of intermediaries (holding the credit card information) in the payment process, the threshold must be as strict as possible, because it represents the unique way of authentication. If this authentication is completed erroneously, then the wrong persons are charged, with no possibility for them to prove the mistakes. On the other hand, when the users have to submit their credit cards' numbers at each purchase, it increases the security level, by adding another identification process. The threshold could then be lowered. However, at each transaction remains the risk for hackers to intercept these credit cards' information. Concerning electronic cash, as the solution of credit cards held in electronic wallets, the more secure those systems will be, the more flexible the thresholds will be made. Nevertheless, the goal of biometrics authentication is to replace all other identification procedures and to make the process as simple as possible for the users. Therefore, as it represents a trustable technique, if biometrics should be used for online commerce, it could help conceiving the payment methods in a more convivial manner.

Globally, regarding electronic commerce, the threshold shouldn't be lessened, because the online business is a very sensible area, for which the key of success is materialized by the exchanges' reliability. Even if the FRR is relatively high and bothers the customers, it is preferable to a higher FAR.

3.2.2 Level of Security

Biometrics applications are diverse and reach various sectors of everyday life. From banking security, to access control, through information system security, immigration procedures, government benefits distribution, national ID systems, etc. [22]. The threshold value is certainly dependent on the level of security desired in an AFIS, regarding its application domain. High-security areas are more likely to employ very high threshold values, for a strict access control, in comparison with the use of biometrics for cellular phone access for instance, as mentioned in the previous chapter.

The concept of adaptable threshold, regarding the system level of security suggests that a single system will permit modification of its acceptance threshold (as an option), based on its application area. In order to do so, the security level has to be quantified. Nonetheless this quantification has to be assessed by the AFIS manufacturers themselves during the system conception, and may not entirely satisfy all the customers. The manufacturers will have to evaluate the different levels of security and assign a specific threshold to each of them. The principal issue for the customers is to know to which level they estimate the security of their systems stand. The manufacturers should indicate precisely the two error rates (FAR and FRR) associated to each threshold, to guide the customers in their choices. It is logical to assume that a “standard” customer will always select the highest value for the threshold. Nevertheless, a “restricted” threshold may be cumbersome for the users (because of the high FRR), especially when the domain protected does not require an exceptionally secure authentication. This scenario will surely happen, when biometrics will have reached all areas of authentication and not only, as for now, limited domains requiring exceptional security.

Threshold value (- to +)

Security Level	FAR %	FRR %
1	0.09	7.2
2	0.05	10.3
3	0.01	12.9

Table 5: Thresholds choice in AFIS X

In Table 5, an example of the level of security selection by the customers, is exposed for an imaginary AFIS. Each level is associated with particular FAR and FRR values that give the precise meanings of these levels. The security level increases with the threshold value, for a more secure and reliable system. Secure and reliable in the sense that the FAR should be as low as possible: the goal is to absolutely forbid the acceptance of impostors, at the expense of a rise in the FRR. An increase of false rejection errors is more disturbing than dangerous, like it is the case with an augmentation of false acceptance errors. In this example, if the customers want the maximum security, they will have to deal with possible repeated tries for a rejected genuine user, but on the other hand, they will be assured to lessen the risks of frauds.

In a few years, when biometrics will be a common, wide accepted and widespread mean of identification, this idea of level of security will be more judicious.

3.2.3 Level of Privacy

This notion of level of privacy is similar to the one of level of security, but better suited to another application of biometrics: the information access, when security is rather related to “area access”. Based on the same model exposed above, customers should be given the choice of selecting the level of privacy related to the AFIS they’re using. Assume both options are presented to the customer: the tuning of both the levels of security and privacy. Then there is redundancy, as both variables are in fact identical regarding the algorithm. They influence the threshold in the same direction: their goal is to perfectly authenticate a user by reinforcing the vigilance with the increase of the acceptance threshold value. To conclude, either it is called security or privacy “tuning”, the feature is the same or only one of both notions should be implemented. In the following, the distinction is not made between both terms.

The level of security adjustment can be interpreted as a tool for varying the “granularity” (i.e. the item size) of the entity of the system. In other words, the customer can choose to base the identification on an individual user scale or rather on a larger scale (group) for commodity.

This concept is slightly subtle in biometrics, in comparison with passwords or smartcards based authentication. Indeed, in biometrics the level of security cannot be adjusted to group level, for manageability purpose. The goal of lowering the level of security from individual user to group level, for instance, is to facilitate the passwords (or smartcards) management in large systems. For example, a single password can be assigned to a particular group of persons (small sections within departments in a company) for data access (same privileges for all users), resources (copy machines), or admittance in certain areas of a site. This is useful when the administrator doesn’t need to know who exactly within the section has utilized the resources, because these resources are not highly valuable, but are reserved only to the section in question. The obvious advantage for administrators in doing so, is that instead of creating individual passwords for a sole purpose (either data access or facilities access, etc.), they can assign a common code to the whole section. Under the assumption naturally, that all of the users have equal authorization for the resources. This is for sure not an optimal situation, in terms of efficient tracking of the resources usage by the personnel in the workplace. The larger the set of users employing the common password is, the more difficult the control will be. Yet, the efficiency of such an authentication system will not be tackled here.

Whatever the efficiency of such systems is, with biometrics this method is inapplicable. As the identification criteria are distinct for each person, there is no possibility to share biometrics characteristics among a group of persons, as it is the case with passwords and smartcards. With these last ones, it is possible to lower the level of security, but still forbid the entrance to unauthorized users, (people who don't belong to the allowed groups) thus maintaining a certain level of control on the system. On the other hand, in biometrics, groups can't be substituted to users. Therefore, the only reasons and consequences of modifying the level of security in biometrics are to influence the FRR and FAR. Either for a more comfortable utilization by the users, (decrease of the level of security) or an improved reliability of the system (degree increase).

The security (or privacy) degree is a legitimate candidate as a criterion for threshold modification. It denotes however, subjectivity, because it is an option completely dependent on the AFIS administrator.

3.3 Images of Poor Quality

Three different types of factors can contribute to create noise on fingerprints images:

– Skin's injuries result in a "*irreproducible contact*" of the finger on the glass platen by altering the ridge structure [22].

– External factors: (dirt, humidity, sweat, etc.) lead to a “*nonuniform contact*”. They prevent the finger from being in a regular contact with the glass platen. Some ridges may not appear, and on the other hand, valleys can be in contact with the platen, when the contrary should occur normally [22].

– Bad scanning equipment: some acquisition devices may not produce a good image resolution.

“Noise” in fingerprints images will either create fake minutiae, or rather remove genuine ones. It can also induce errors in the minutiae position and location. For very poor quality images, the normal threshold will not be appropriate because a significant amount of minutiae will not be exploitable. Therefore, the decision could be taken in such cases (comparisons of poor quality images), to lower the threshold, to still pursue users authentication.

Here again, the same question appears: Does the lack of minutiae constitute a valid reason for threshold modification? The answer is **No**. It can be done for commodity purposes, but it undeniably weakens the whole system. Yet, the decision depends on the AFIS application and its level of security. How to solve the problem of images quality then? The solutions differ according to the causes of the noise:

– *Skins related problems*: in prevision of possible future injuries, fingerprints should be taken for two or three fingers for each user. These extra prints don’t have to be stored in the same database than the current one, the system can allow secondary databases as kind of “rescue databases” for such situations.

– *Environmental conditions*: (humidity, dirt, sweat, etc.). People can get into simple good habits to anticipate these errors prior the finger scanning: fingers can be cleaned to eliminate sweat or dirt; or alcohol can be applied on fingertips against hands’ dryness [56].

– *Equipment quality*: Investments should be made for high quality scanning instruments.

When for a reason or another the system is still in presence of a poor quality image, then depending on the amount of noise, it will certainly be unable to recognize identical fingerprints. It is wiser to reject the users, if their input images are not “readable” than to try to lessen the acceptance threshold.

Concerning the template image, a quality threshold should be applied to forbid the enrollment of a user, based on a non-exploitable image.

Obviously, this other criterion is once again not relevant for threshold modification.

Among the seven possible parameters, classified in three categories, eligible for the threshold's adaptability, only two of them, namely the minutiae's type and the level of security criteria are indeed suitable, for making an AFIS system more flexible.

Summary and Transition

This chapter has discussed, through various potential criteria, the validity of the threshold adaptability in an AFIS. It appears that this notion is completely rational and indeed desirable in authentication systems, to improve the universal character of such a technique. By allowing its adjustment to the systems or sites it should protect, the AFIS solution will be perceived as more convenient to customers, in comparison with other authentication techniques. Indeed, it will combine robustness, reliability and ease of use, at a lower cost (AFIS).

The next chapter will try to define a concrete way of estimating and calculating the threshold value, regarding the criteria found relevant for its adaptation.

Chapter 4: Threshold Computation

The threshold computation is completely related to the algorithm defined for the minutiae matching in the AFIS. Essentially, each fingerprint-based authentication system will base its technique on a certain pattern of the fingerprint that will be exploited in a certain manner. Hence, the threshold computations and values vary from a system to another. To be able to reach a consensus regarding the definition of a general set of rules for threshold adaptation, it is necessary to build these rules on an element common to all those systems. When talking about fingerprint authentication, the first notion to be thought of is minutia points. However this is not necessarily the factor of reference in every method. Some of those finger-based identification algorithms either don't use minutiae for authentication [30], [32], [38], or use them but only as an intermediary component of the matching process [31]. Nevertheless, the minutia points are the most widespread pattern used for fingerprint identification. Consequently, in the following, the formulas will be based on the number of minutia points required for a reliable result.

Now that a number of criteria authorizing the threshold modification have been determined, the aim of this chapter is to effectively perform this adaptation, by defining a set of common rules applicable by various AFIS using minutia points for identification. A further extrapolation to other biometrics techniques will then be considered.

As previously explained, the minimum number of minutiae detected for a valid authentication, is not a determined number for which everyone agrees on. However, as the number of twelve is usually mentioned, it will be referred in the remainder, as the "standard" number of minutiae, corresponding to an average or normal threshold value. When the threshold value will have to be adjusted for a specific case (a more severe or more flexible system), then the new value will be computed in terms of number of additional or deductible minutia points necessary. The main issue here is to quantify the degree of flexibility of the system. When a strict system is requested, then which level of strictness shall be implemented? How many minutiae points correspond to this level?

Only two criteria were found appropriate for the threshold adjustment: the level of security and the minutia points type. Both present various scales in their interpretation and application to the system. Therefore, multiple rules must be conceived.

4.1 The Level of security Criterion

The estimation of the level of security of a system is a subjective notion, left to the judgment of first the AFIS designer, and then the administrator at the client's level. The only tools for appreciating the consequences of the variations of this concept on the system reliability, are both the FAR and the FRR. They give a concrete idea of how the procedure behaves in terms of users acceptance.

As the notion is subjective, not to say fuzzy, the fuzzy logic theory seems to be the most adapted method to estimate the different threshold values.

4.1.1 Fuzzy Logic: Principles

The fuzzy logic has been elaborated as an answer to human reasoning, concepts for which a precise definition does not appear clearly [57]. For instance, the perception of an individual height is "fuzzy" because the limit between shortness and tallness is unclear. Therefore, for this type of reasoning, fuzzy logic provides a scheme to find out computable responses. The Fuzzy Logic (FL) method was imagined by Lotfi Zadeh, professor at the University of California at Berkley. "*FL provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, imprecise, noisy, or missing input information*" [58]. FL has been conceived in a spirit of flexibility and adaptability. It tries to match as precisely as possible, human logic to solve problems, just faster. Therefore, it is particularly suited for control systems, small or large, and can be used at both the hardware and software levels. It is based on a set of IF-THEN rules defined at the beginning of the procedure to formulate the questions as simply as possible, rather than trying to operate in a mathematical way. The typical example is a temperature controller system. The fuzzy thermostat unlike an ordinary one will not work as an on-off switch but rather will continuously adjust the temperature, regarding the feedback received [59].

FL operates through three main steps:

– Fuzzification of the inputs in fuzzy terms

– Inference from the rules, to compute the outputs

– Defuzzification of the fuzzy outputs into crisp values

To help explain the method, the thermostat example will be employed through the entire process. The FL starts by establishing IF-THEN based rules to define the output answers according to the system input conditions. The rules concerning this example follow [59]:

– **Rule 1**: IF *temperature* IS *cold* THEN *fan_speed* IS *high*

– **Rule 2**: IF *temperature* IS *cool* THEN *fan_speed* IS *medium*

– **Rule 3**: IF *temperature* IS *warm* THEN *fan_speed* IS *low*

– **Rule 4**: IF *temperature* IS *hot* THEN *fan_speed* IS *zero*

The first step is the fuzzification of the conditions (input) in fuzzy terms.

4.1.1.1 Fuzzification

The transformation of the rules conditions in fuzzy concepts is done by the membership functions. A membership function will represent graphically the term or notion expressed in the conditions of the rules and will weigh it according to the membership values. A membership value indicates for a specific value of the function (on the X-axis) its degree of belonging to the concept (membership value on the Y-axis). The ordinary shape of a membership function is the triangular one (Figure 10), but other have also been used (bell, trapezoidal, exponential) [58].

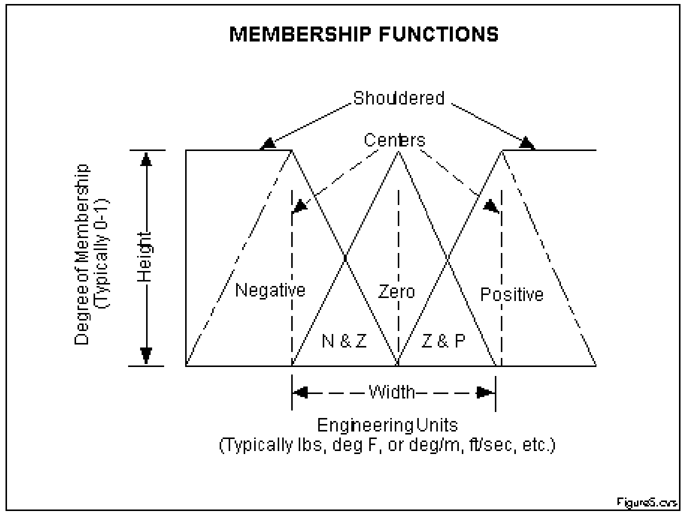


Figure 10: Features of the membership function [58]

The Figure 11, illustrating the fuzzification step, presents four membership functions symbolizing the four concepts expressed in the rules conditions (cold, cool, warm, hot).

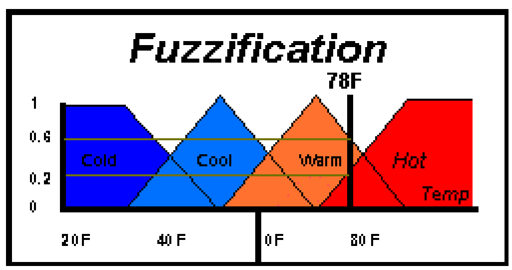


Figure 11: Fuzzification of the temperature concept [59]

As brought up earlier, the fuzzy thermostat does not resemble the traditional one, in the sense that it does not have fixed limits for the different states, instead, the different temperature conditions overlapped themselves regarding the values. Therefore, the value 78F is fuzzified in *warm* with a membership value of 0.6 and *hot* with a membership value of 0.2. This representation is closer to the human logic.

4.1.1.2 Inference

During this step, only the rules with the conditions equivalent to the fuzzified values are considered. For instance, in this example, only rules 3 and 4 will fire, because they refer to warm and hot temperature (78F is warm (0.6) and hot (0.2)).

After selecting the rules, the membership values then have to be propagated to the conclusions of these rules. In Rule 3, the fan_speed will be lowered at 60% and from Rule 4 the fan_speed will be turned off at 20%. These results are not really meaningful before the defuzzification stage that will indicate in crisp value, the appropriate fan_speed.

4.1.1.3 Defuzzification

One defuzzification method widely used is the one computing the searched value as the center of gravity of the membership values of the outcomes.

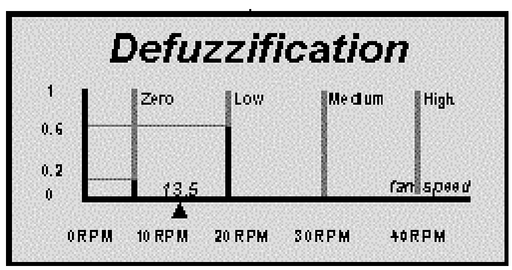


Figure 12: Defuzzification [59]

In the defuzzification step (Figure 12), the output membership functions are represented, rather than the input values in the fuzzification step. For each different outcome, the result found in the inference step is reported: *low* is assigned the value 0.6 and *zero,* the value 0.2.Both medium and high outcomes, are considered null, as their corresponding rules didn't fire. The X-axis now indicates the variable "fan_speed" instead of the temperature.

For each outcome, the fan speed value that corresponds to the maximum membership value for the function is selected. For instance for the *low* function, a speed around 20RPM (an estimation regarding the graph, in the absence of precise data) gives the highest membership value (1) for the function. The method used to calculate the correct fan speed value, is called the "ROOT-SUM-SQUARE" method [58] and computes the searched value as the "*fuzzy centroid*" or "*center of gravity*" [57] of the membership values.

(HV_zero*MV_zero + HV_low*MV_low + HV_medium*MV_medium + HV_high*MV_high) / (MV_zero + MV_low + MV_medium + MV_high)

HV_zero is the fan speed value corresponding to the highest membership value in function *zero* (HV_zero is slightly inferior to 10 RPM). MV_zero is the membership values found in the inference step for each outcome (MV_zero=0.2). The same logic is valid for the other functions.

The result of the computation gives the best fan speed for a temperature of 78F (13.5 RPM).

These three different stages will now be applied to the level of security criterion.

4.1.2 Application on the Level of Security

The problem to be solved is to determine the numbers of minutiae that correspond to the different levels of security. Another assumption made is that the AFIS offers five levels for the system security. The *normal* one corresponding to the twelve minutia points, the *very low*, the *low*, the *high* and the *very high* one. Here, the terms or concepts of the rules conditions will be labeled as security levels, but implied, are the FAR values of the system related to these levels of security. The FRR don't need to be considered, because regarding the security of an AFIS, the only concern is to forbid the system entrance to impostors. Thus, for any value of FRR, it is the associated FAR that really determines the system level of security. The rejection rates are then omitted. "IF X THEN Y" type of rules are again utilized. The questions raised will resemble the following: *With a Level of security X (equivalent* *to a FAR value Y) what is the corresponding number of minutiae?* The related rules base will contain five rules: *IF Security_Level is very high/ high/ normal/ low/ very low THEN minutia_number is very high/ high/ normal/ low/ very low*. No value is specified in the rules, only imprecise notions (low, normal, high, etc.), then when needed, concrete values will be provided to interrogate the system on the exact number of minutia solicited. There are five distinct estimations of the rate, showing the five possible levels of security, thus there will be five rules:

– **Rule 1**: IF S*ecurity_Level is very high* THEN *minutia_number is very high*
– **Rule 2**: IF *Security_Level is high* THEN *minutia_number is high*
– **Rule 3**: IF *Security_Level is normal* THEN *minutia_number is normal*
– **Rule 4**: IF *Security_Level is low* THEN *minutia_number is low*
– **Rule 5**: IF *Security_Level is very low* THEN *minutia_number is very low*

For the purpose of the fuzzification, the membership functions of the five input concepts *very low, low, normal, high* and *very high* (IF clauses) have to be represented in terms of FAR. The values of FAR used in Figure 13 to build the membership functions are based on assumptions and examples of FAR, taken from existing AFIS. Nonetheless, their estimations try to match as closely as possible reality. The FAR values and the levels of Security vary in opposite ways. Only two situations are worth using FL for the level of security: the low and high levels of security (high and low FAR) conditions. The method will be applied for only one of these two conditions and will ignore the rest, because the procedure is always the same. The goal is just to demonstrate that the FL method can be utilized for defining the threshold associated to a particular level of security in an AFIS.

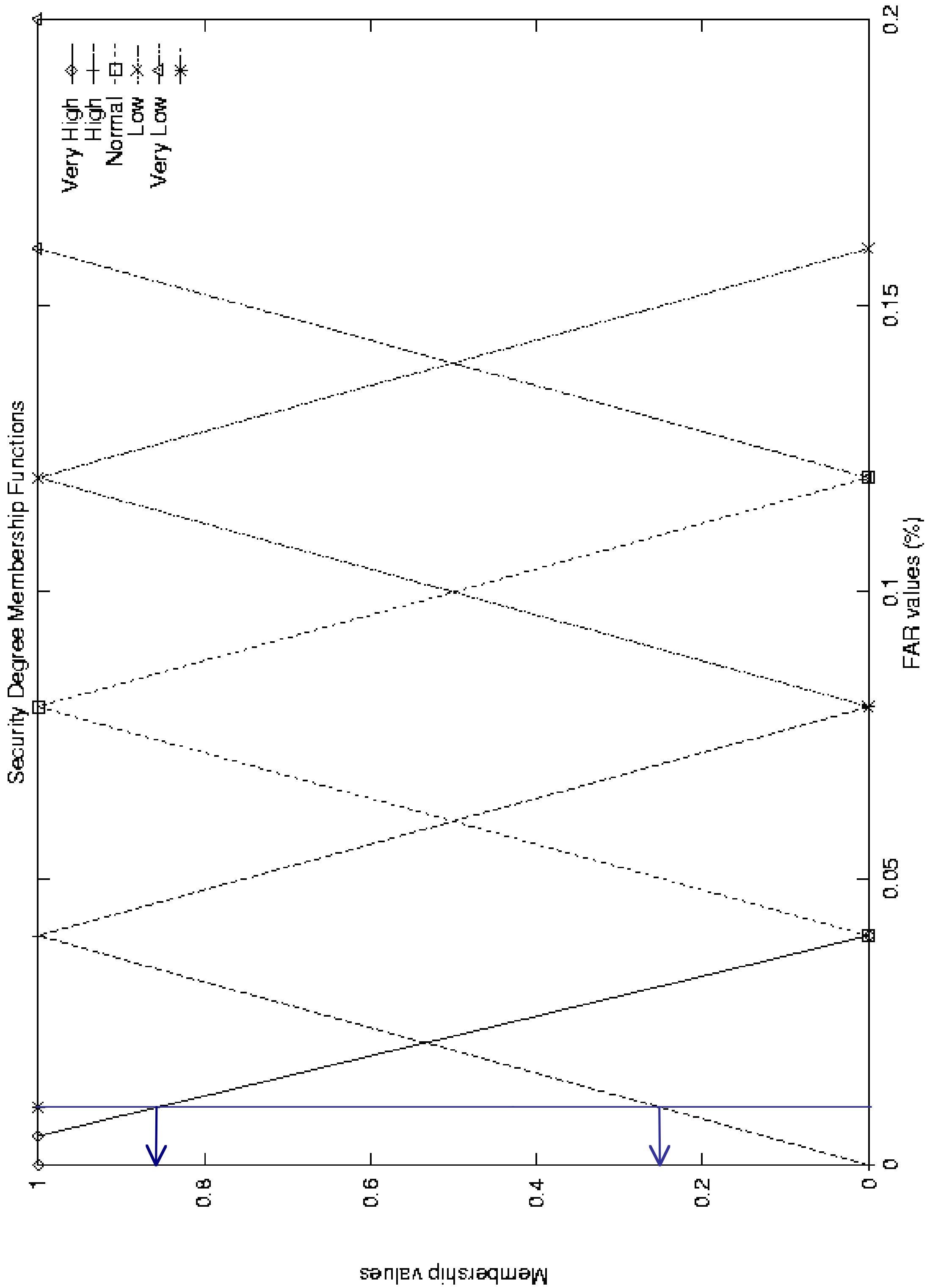


Figure 13: Levels of Security Membership Functions

A high level of security is equivalent to a low FAR. For this example, the FAR is equal to 0.010 %. The value is indicated on the graph as a straight line.

– The **fuzzification** stage transforms the FAR value of 0.010 in "Security_Level is high" with a membership value of 0.25 and "Security_Level is very high" with a membership value of 0.86.

– The **inference** step selects Rules 4 and 5 and leads to the outcomes: the "minutia_number is high" at 25% and the "minutia_number is very high" at 86%.

– During **defuzzification**, the fuzzy values are converted again, and the final value is 19 *minutiae*. The formula used is [(20*0.86) + (16*0.25) / (0.86+0.25)].

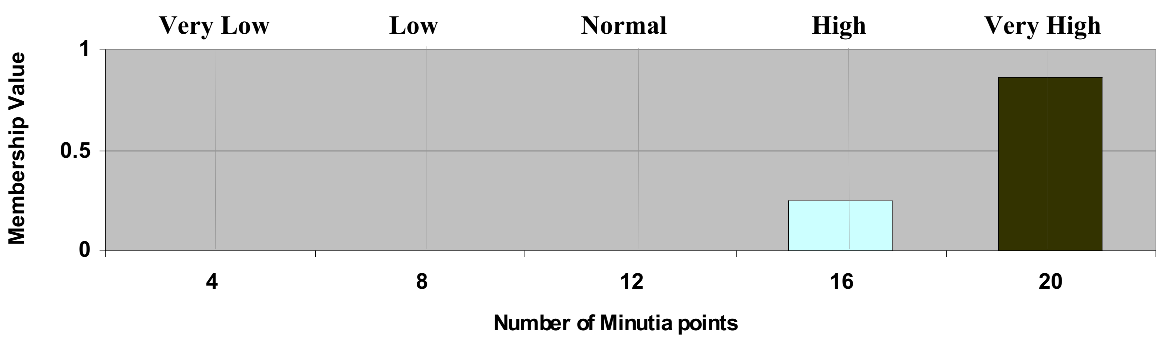


Figure 14: Minutiae Number membership functions

Nineteen is the number of matched minutia points defined for the threshold dedicated to an AFIS with a high level of security.

In conclusion, here is a way for AFIS designers to include in their systems the level of security tuning, as an option given to the its administrator (client side). This threshold modification is facilitated by the application of the FL method. Many of the existing AFIS in the market have already provided the adjustment of the level of security by the customers. Generally, five levels are available, as for Biometrics Identification Inc. *Veriprint* serie [60], [61]. The ABC *Biomouse* permits the FAR configuration, which is exactly the same feature than the level of security tuning [48]. The systems' descriptions however don't indicate the kind of algorithms in use for the thresholds' modification. Nevertheless, the Fuzzy Logic constitutes an appropriate and realistic technique as it can be implemented in both hardware and software.

The other serious criterion for threshold modification, the minutiae type, will use another technique for the threshold's adaptation.

4.2 The Minutia's Type Criterion

The data used in this section are the data presented in the article of Osterburg, Parthasarathy, Raghavan and Sclove [28]. These data were also employed in the section entitled "Minutia's Type", exposing the validity of this criterion for threshold's tuning.

4.2.1 The "Rarity Weight" Variable

The purpose of the present discussion is to determine, for a precise set of minutia points' types, the appropriate thresholds that can be assigned to them. Each type, as seen earlier, exhibits a certain probability of occurrence in the fingerprints. For sure, these probabilities relate on studies and therefore the numbers cannot be taken as "established" numbers. They only reflect and give appraisals of the different minutiae's distributions, for the particular images processed in the given study.

For each occurrence probability, a weight is computed as the negative log of the probability. This "weight" variable evaluates for a given type, its ability to lead to the correct identification of a person. The greater this weight is for a particular minutia's type, the more information, in terms of identification capability, it brings for the authentication. Table 6 shows the weight associated to each occurrence probability [28]. For a given configuration, the sum of all the points' weights ($[-\Sigma_i k_i \log_{10} p_i]$ or $[\Sigma_i w_i]$) reflects the validity of this configuration as a trustable candidate for identification. In other words it indicates, whether or not a positive authentication can be concluded, if all the configuration points match in both the input and the template.

Grade	**Minutia type**	**Estimated Occurrence probability (p_i)**	**Weight ($w_i = -\log_{10} p_i$).**
1st	Empty Cell	0.766	0.116
2nd	Ridge ending	0.0832	1.08
3rd	Ridge bifurcation	0.0382	1.42
4th	Island	0.0177	1.75
5th	Dot	0.0151	1.82
6th	Bridge	0.0122	1.91
7th	Spur	0.00745	2.13
8th	Lake	0.00640	2.19
9th	Delta	0.00198	2.70
10th	Double bifurcation	0.00140	2.85
11th	Trifurcation	0.000582	3.24

Table 6: Minutia Types' Weights

In Table 6, the trifurcation as the rarest type possesses the greater weight. The conclusion after computing the sum of the weights is based on a comparison once again with a threshold. This solution opens a large number of possibilities. Contrary to the "Minutia's Type" section, not only each type will define a particular value for the threshold, in terms of numbers of points needed, but now it is the *nature* of the additional points that would be relevant, independently of their total number. In short, for each minutia's type, several configurations would be acceptable, as long as their weights' sum equals or is superior to the threshold. This approach doesn't focus any longer on the numbers of points required, but rather on their types, once more. It appears as a recursive process. A more flexible and maybe more intelligent method than the one previously considered. However, its complexity degree when applying it to an AFIS is much higher, because of the infinite number of possible solutions. Nevertheless, this solution is closely akin to the first one stated. Indeed, even if the threshold is conceived following a logic of number of points, at a certain moment, the following question will certainly raise:

“Which points?”. Assume that, given a particular minutia’s type, it has been resolved that only x further minutiae should matched. Then this answer is in fact incomplete and one could ask if these x minutiae could be of any type. From the most common one?” It surely makes a difference if some of the additional minutiae are also very rare points, because it could lessen the threshold once more. Furthermore, knowing that each type has a different effect on the threshold, it would be more judicious to exploit this property entirely, and not only partially. Hence, eventually, the solution brought by the “weight” method resurfaces.

The complexity problem for the AFIS implementation of such an approach is not as arduous as it seems. The algorithm does not need to know all the configurations leading to the “threshold sum”, which is of course impossible, as the number is infinite. It will only have to worry about the total sum of the matched points’ weights. Now the question is to find out, how to compute this threshold sum.

Before going further, a remark should be pointed out. All the reasoning is done on the occurrence probability of the minutiae. The aspect of points’ matching is never obviously exposed, and thus the parallel between the two notions (occurrence and matching) may seem unclear to the reader. Indeed, the points’ matching is an implicit condition. The logic is the following: knowing that a configuration c, of points, has a probability p of occurring in a fingerprint image; if the input and template images match on these configuration points, then p indicates if it is correct to conclude a positive authentication. The condition that both images present the same points at the same location is never really explicit, but otherwise, the reasoning is illogical.

4.2.2 A Possible Algorithm

The idea of this method is to make it as simple and intuitive as possible, without any essential restrictions for the designers. For each particular minutia’s type, its capability of yielding a trustable authentication will be evaluated. For the definition of the threshold sum, in a concern of portability, we’ll state as the starting rule, that it will be equal to the sum of the 12 most frequent points’ weights ([12 w_i] or [-12

$\log_{10} p_i$]). These frequent points will most likely be the ridge endings. To permit its implementation in any AFIS, the method will define this threshold sum, as well as the occurrence probability of each minutia' type[8], according to the AFIS images database. This database is filled in with fingerprint image templates, resulting from the users' enrollment. The computations will be done once, before the setting up of the AFIS.

The method will now be applied to the algorithm described in the Section "2.1.3 Minutiae's Type". This algorithm depicted the matching stage of an AFIS implementing threshold adaptation, regarding the minutia's type. Even though, this algorithm is still in accordance with the logic of the current method, there is still one single difference. Indeed, the threshold now does not have the same significance. In its old version, it represented a number of matching points, related to the type of the first minutiae's match. This number was decremented at each match and the algorithm stopped when either the threshold reached zero, or when one of the points' lists was at the end. Here, this threshold is a sum of weights. Thus, at each match, the weight of the matched minutiae will be added to the current weights' sum for the given configuration. The stop conditions are either the reaching or exceeding of the threshold sum, or the end of one of the minutiae's lists. Another advantage of this algorithm is that there is no more need for the comparison of all the points in the configuration. As soon as the sum will reach the value of the threshold sum, the algorithm will stop and will be able to conclude to a positive identification. As these points are arranged in descending order, the more meaningful points will be first tested and will save time for the authentication process. Hence, the new algorithm is:

Declaration of the variables used in this algorithm:

i: Minutia in input list

j: Minutia in template list

Wi: Weight of the input minutia i processed

Wj: Weight of the template minutia j processed

S: current weights' sum

S_T: Threshold sum

[8] For ease of use, the AFIS administrator could use only the ten types named in the presented article.

Nx = Number of matched points (threshold) associated with the minutia x's type.

```
i=1; j=1; S=0; S_T=12*Wc; ("c" representing the most common type)
while (S<S_T) and (i <= EOF_Input_List) and (j <= EOF_Template_List)
        if (Wi=Wj) then //same minutia's type
            Try to match both points;
            if (match) then
                S=S+Wi; //current sum increased by minutia's weight
            endif
            Select next (i, j) to compare
        endif
end while
```

The algorithm will now be executed with the following example, a configuration of points (sorted in descending order) and their associated weights indicated in Table 6:

- 1 Trifurcation (w=3.24)
- 1 Spur (w=2.13)
- 1 Bridge (w=1.91)
- 3 Islands (w=1.75)
- 5 Ridge Bifurcations (w=1.42)[9]

It is supposed that every minutia comparison with the corresponding point in the template is a match. The only concern is to determine the number and types of points, sufficient for a correct authentication.

Except for the empty cell type that does not exist in the current method, the most common type of points is the ridge ending one, which has a weight of 1.08. Therefore, the threshold sum equals 12.96 (12*1.08).

1. The process starts with the first point in the list, the trifurcation. According to the assumptions previously exposed, it matches the trifurcation point also present in the template. The configuration sum at this point is *S=3.24*.

[9] The weight values are for one occurrence of each type

2. It continues with the spur and $S = 5.37$ (3.24+2.13)
3. The bridge point is also identical, then $S = 7.28$. The sum is still inferior to the threshold one (12.96) and none of the list has reached the end. Because, it is supposed that the template possesses the same points as the input fingerprint image.
4. The three islands increase the value of S, that now equals *12.53* (=7.28 + 1.75 + 1.75 + 1.75). None of the condition has yet been satisfied to stop the algorithm.
5. The first bifurcation's match will produce a sum of *13.95*. It now exceeds the threshold value and will cause the algorithm to stop.

In conclusion, seven points were enough to accurately identify a person, due to the presence of rare points.

This simple and "portable" solution could be easily implemented in any AFIS that would like to perform this kind of optimization.

In fact, the flexibility concept was applied to a superior level than that of the threshold. It was not the threshold that was modified anymore, but rather the configurations of points, which "grades" reached the fixed threshold value. One could argue that the technique wasn't the same any longer and that it couldn't be seen as an example of threshold adaptability. The answer to that probable critic is "Yes, the threshold has been actually adapted!" This threshold is in fact expressed in terms of number of points needed for a correct authentication and not in terms of the configurations' weights. Thus, as illustrated, many configurations with different numbers of points are acceptable, and these combinations represent the valid thresholds. This case shows the different connotations of the threshold notion.

Summary and Transition

This chapter has proposed two different techniques for adaptable thresholds' computations. The Fuzzy Logic method is useful in situations where notions are subjective, hardly quantifiable and their limits imprecise. It is perfectly suitable for the settings of the levels of security, in terms of accurate values for the threshold. The algorithm developed for the minutia's type criterion fits more in the logic of a global method, appropriate either, for the normal or the unusual cases.

The following chapter establishes a generic method for threshold's adaptability. The goal is to define a method, as general as possible, usable by any biometric characteristic to determine flexible thresholds.

Chapter 5: Generic Method for Threshold's Adaptability in Biometric Authentication Systems

The aim of this work is to demonstrate the procedure for possibly adjusting a biometric authentication system to several particular situations, for a more efficient and smarter usage. This adjustment can only take place at the threshold's level, because the threshold is the only "software tool" that can be manipulated in real-time, by the customers. Of course, this manipulation will be done with external parameters that will cause the threshold's modification.

The main question that should be asked before modifying a threshold is: "*What allows us to declare that a threshold is adaptable?*" This threshold's adjustment should be performed while maintaining the same level of reliability for the system. It was demonstrated earlier in this thesis that it was also possible to adapt the threshold, to reach the level of security required by the client. Still, this is a particular situation because it completely changes the goal of the whole system. In this chapter, the main focus is the modification of the threshold, in an attempt to simplify and accelerate the authentication process. This should be done without interfering in any way in the overall product's performance.

In this chapter, I will present a procedure that should be followed to exploit and evaluate a biometric trait, in order to possibly adapt the threshold. It will close by speculating on a further matter, related to the matching stage and the data format.

5.1 The Procedure

As explained above, there are many biometric characteristics usable for automatic authentication. Despite their differences, the methodologies for defining a threshold's adaptability are similar. Therefore, it is possible to establish one scheme, applicable to any characteristics.

5.1.1 The Feature and its Representations

The feature is taken as a whole and called F. F can be any biometric characteristic: a face, a hand, an iris, a retina, a fingerprint, etc. The major difficulty in establishing a generic method is due to the diverse possible features' representations. Most of the authentication systems include a transformation phase during which the patterns to be tested are converted into more suitable forms for comparison with the templates. These forms involve digital representations (gray-level, colored or binary images), Fourier representations [62], etc. The aim of this modification is to permit the matching process by computers.

In order to have a brief survey of the possible feature representations, existing data formats are reported for several biometric traits (the physiological, not the behavioral ones), used in automatic authentication systems.

Face

In most of the automatic face-based authentication systems, the face is first decomposed into its different local features. The eyes, the nose and the mouth are the most important ones, but some systems may include additional features. The face decomposition is usually a geometrical process. The point to remember for face authentication is that, most of the time it's a mathematical procedure, either in the data transformation or during the matching stage. Therefore, the data can be mathematical formulas [63], geometrical data [64], graphs [65], etc.

Facial thermograms are digitized for computer processing [43]. Mathematical procedures, again, are required for the matching.

Fingerprints

This biometric trait has already been studied in detail and thus will not be analyzed once more. It is assumed that the data representations are digital images, processed to extract the minutia points.

Hand Geometry

This characteristic is scanned to obtain a one-dimension or multi-dimensional representation of the hand. Three-dimension images are actually preferred, because they allow the capture of more features. The length, the width and the thickness of the hand and fingers can be compared instead of just the hand palm pattern. The images are also transformed in mathematical templates [66]. Usually, when it comes to elements' measurements, the pattern has a mathematical representation, associating all the values found. Mathematical templates and inputs are easy to compare, because it's a logic of "all-or-nothing". Small margins of errors may still be permitted, because of the subtle characteristic variations over time.

Vascular Pattern (Hand Vein and Retina)

The blood vessels pattern is used for these two traits: hand vein and retina. This vascular signature is captured by camera and the images are transformed in internal representations, specific to each system. For the back of the hand veins [49], the images are binarized and processed like the fingerprint images.

Other Patterns

The iris pattern is the tissue's texture. It includes the vasculature, as well as other elements. "*The random patterns of the iris are the equivalent of a complex human barcode, created by a tangled meshwork of connective tissue and other visible features*." Given the amount of information provided by the complex network of vessels and tissues, the images are usually transformed in mathematical data. One of the iris' internal representations, the IrisCode, developed by IriScan [40], is a stream of 256 bytes of information (when compressed). It allows evaluating the iris information density at 3.4 bits per square millimeter. It is obtained by mathematical demodulating operations that extract the two-dimensional modulations of the iris patterns.

For the authentication purpose, a fragment of F will be selected, for the comparison with the template. This special part is called G. The reason for introducing G, is that it may be more efficient to process a smaller but more significant region of the feature, than to consider the entire F. This will save the processing time of a larger but less meaningful area. This logic of course, makes only sense if it is supposed that the inequality sought-after exists in all the cases.

5.1.2 The Choice of G

Usually, the feature partitioning is allowed by the observation of unequal repartitions of the information, on it (when more meaningful areas than others are detected). Yet, this segmentation is not a valid concept for all the traits. Concerning the iris trait, unlike the fingerprint for instance, the representation of the whole feature is used for the matching. The idea of selecting the most relevant zone is not appropriate, in this case. This is due to the amount of details in the iris pattern, formed by the various elements' types. It is in fact, the combinations of all the small features, that guarantee the uniqueness of the iris trait. "*No two irises are alike in their mathematical details, even among identical (monozygotic) twins*" [40].

The choice of G takes on two aspects: on the one hand, its geographical localization, "Where on the feature F is it more judicious to select G?" and on the other hand, its aspect "How G is formed?" Concerning this last point (Figure 15), G can either be composed of a continuous part of F, or it can consist of an assortment of subsets of F. In this latter, $G = \bigcup_i G_i$

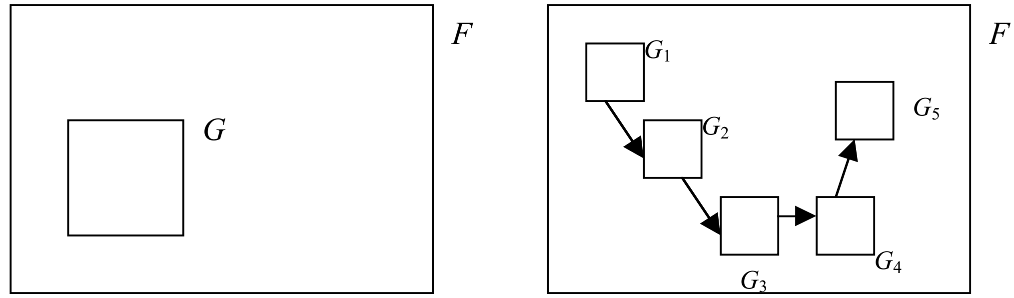


Figure 15: The Organization of *G*

This organization of G is completely dependent on the characteristic itself. For a face-based authentication, the subsets' solution would be preferred, because the face characteristic is usually represented by a set of its different features, independent one from another. However, with a fingerprint-based identification, the area considered will be the pattern area, which is one complete and continuous "block" on the whole fingerprint.

Regarding the geographical localization, it is related to the amount and the quality of the information found in the area. In other words, the system should detect the most "interesting" regions, the ones exposing the most exploitable data. This notion of relevance means that, it is not the entire *F* that is scrupulously compared to the templates, pixel by pixel, or bit by bit. Rather, critical areas are extracted and matched. The unequal information distribution can be symbolized by the various categories of the elements constituting the feature. Some of them may be more significant than other. This is portrayed by the face characteristic. "The most interesting regions" are the eyes, the nose and the mouth at least. However, for other traits that use a pattern where all elements are from the same category (blood vessels pattern, minutia pattern, etc), the selection of the appropriate regions is based on other criteria, like their types for instance.

Concerning identification systems based on face and hand geometry, it should be pointed out that these cases are slightly different from the majority of the biometric systems. Indeed, in these situations the problem of selecting a relevant area does not exist as presented here. Whatever the face or the hand to authenticate, the same features will always be selected. For the hand geometry, several definite properties or parts of the hand are measured. Therefore, for these kind of systems, the idea of extracting a specific *G*, as a special part of *F* remains, but the algorithm does not have to seek for this *G*, it has been programmed by the user to select determined regions.

Regarding the biometric methods beside the ones based on face and hand geometry, it is not sufficient to detect the differences in the repartitions. The most important point is the possibility to quantify them. Hence, the next steps in the reasoning is to find out, first, how to find the potential critical areas, the "*G*" sections, and second, how to evaluate and grade them. The answers to both questions lie in the definition of a function (EVAL(G)) that will indicate the degree of complexity of the *Gs*. The best logic to detect the most significant zones is to examine the entire *F*, by considering EVAL() as the selection parameter. In order to do so, the evaluation criteria need to be determined. In other words, the question "What can EVAL() measure in the *G* sets?" has to be solved. This information relevance evaluation will not be based on the same criteria, depending on the biometric characteristics and the features' representations. Another way of proceeding would be to select multiple *Gs*, at random, and then chose the one with the best value for EVAL(). A reasonable number of attempts could be fixed to keep the process under control. However, as this solution is clearly not optimal, because of the risks to miss the most pertinent zones, the first one expressed is preferable.

5.1.3 The EVAL() Function

The EVAL() function can represent many concepts for the information evaluation, depending on the data and their representations. There are two notions associated with this function: the determination of suitable criteria for finding and quantifying the interesting areas and the definition of the techniques employed to analyze the feature *F* (depending on the criterion selected). The selection of both the criteria and the techniques relies on certain parameters.
The data processing techniques are associated to the features representations, which are:

- Digital images
- Mathematical representations
- Internal Codes of bits

The criteria depend on the biometric characteristic analyzed:

- Fingerprint
- Eye
    - Vascular pattern of the retina
    - Iris' texture

- Face
- Hand
    - Hand geometry
    - Hand Veins

For some biometric traits, several representations may be possible and thus the EVAL() function will change regarding the representation chosen.

At first, the techniques are detailed for the three data layouts, subsequently the exploitable criteria are studied.

5.1.3.1 The Data Analysis Techniques

The features can be stored in computers as images, mathematical data or internal codes of bits specific to each system. In all cases, the information are digital, for computer matching.

Digital Images

In digital representations, the bit streams materialize the pixel's color intensity or gray level. In this case, how is it possible to detect relevant parts of the feature? To answer this question, a brief description of the image analysis principles is helpful for the understanding of digital images' processing [33]. In image analysis, the normal flow (independently of the image format: gray-level, binary or skeleton) is illustrated in Figure 16.

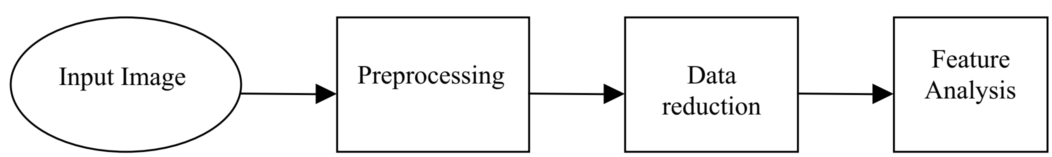


Figure 16 : Image Analysis [33]

• Preprocessing

This deals with unnecessary information elimination, (noise, irrelevant part of the image, etc.) or location of interesting regions in the image, for subsequent processing (zoom on a specific area, image translation, rotation, enlargement, shrinkage, etc.). However, this regions' location assumes that the content nature of the images is known. The algorithm is then written to focus on particular regions, known to be present in all the images processed. For instance, for the processing of face images, the system will be conceived to zoom on the central part of the image. This preprocessing phase is the programming of a repetitive and invariant task that should be performed on each image: "*to eliminate borders from the images that had been digitized from film (the film frames)*". This is not, as brought up in this chapter, the discovery of variable characteristics that define the region relevance. At the end of this stage, the system has outlined a "subimage" within the original one that represents its region of interest for the subsequent manipulations.

• Data Reduction

This stage includes many operations, such as edge detection, image transforms, segmentation and feature extraction. These operations help transform the low level image representation (set of independent pixels) into a higher and more explicit one (groups of pixels representing features), as shown in Figure 17. The edge detection locates the edges and the lines in the images, to discover the objects' boundaries. The image segmentation measures the homogeneity, or the contrast of the gray-level, the color or the texture within the boundaries, to divide the image into regions corresponding to objects. The image transform decomposes the image into spectrums, based on the spatial frequency, which is the brightness change frequency in an image. It is then easier to extract the features (or objects) for analysis (feature extraction operation).

The objects' localization at the end of the feature extraction means that, objects have been discerned as entities and separated one from the other. However, they haven't been recognized yet. In other words, the algorithm knows that certain regions of the image correspond to distinct objects, but it doesn't know yet, to which objects exactly. This step is the goal of the next stage, the feature analysis, which examines and evaluates the features for the purpose of an application.

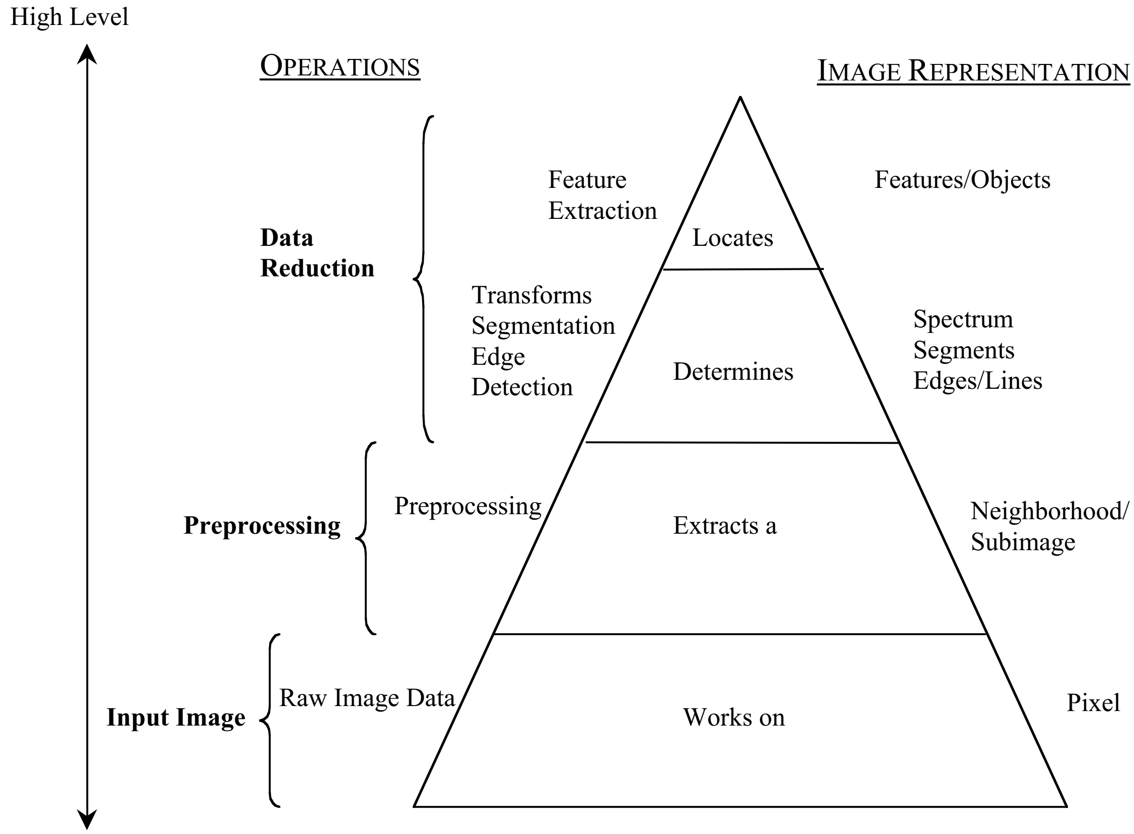


Figure 17: The Hierarchical Image Pyramid (adapted from [33])

- Feature analysis

The feature analysis is a pattern recognition matter. It will attempt to correctly classify each object, by choosing properties that are similar and stable for objects within the same class and different for objects in different classes. There are two approaches for classifying an object [67]: the structural and the statistical one. The statistical solution is based on observation of a set of objects of the same nature. The study of the measures of all the possible properties defines the more apropos ones, (stable within a class and highly fluctuating between classes), that will be used in the classification process. The structural technique considers that "*objects are* *constructed from smaller components using a set of rules*”. Therefore, the main issue when examining an object is to define its components and establish the relationships between them. The representations of these relations will then be analyzed to check if they are in accordance with the basic structure of the object. Both solutions are variations of the template matching process.

In the remaining it is assumed that the image analysis has been completed and that the objects (minutiae, blood vessels, face elements, etc.), have been located and identified in the image.

An important point to understand in computer vision is that the algorithms are application-dependent. For each system developed, the classification properties will vary, regarding how each application will further utilize the objects found.

- Illustration with the fingerprint feature

The processing of a fingerprint image has already been explicated in its main lines, in the section “Description of a Standard Minutia-Based Fingerprint-Verification System” of the second chapter. In the current subsection, the issue will rather be to know how the minutia points are differentiated from the ridges, in the images. It concerns the feature analysis step. As previously explained, the pattern recognition process will select “distinguishing” properties for the objects. Concerning the minutia points, the properties will be related to the points’ shapes. The structural approach is then better suited than the statistical one. Indeed, the minutia’ shapes are not rigid, it’s rather the sub elements’ relationships that are invariant for objects of the same type.

The minutia points are points where ridges terminate, change direction, are broken, enclosed (by other ridges) or interrupted on different locations. Therefore, an intelligent approach for minutia’s type identification would be to follow the ridges until noticing a change in their flow. This is a method already developed in the implementation of an existing AFIS [37]. However, the algorithm only seeks for ridge endings and ridge bifurcations (the most common), as most of the AFIS. This is not surprising given both, the way image processing operates and the structure of the other minutia types. The difficulty in identifying them lies in the fact that the minutiae are not delimited objects. Indeed, most of the time the analysis of the surrounding area is essential to correctly classify a point. Hence, the most efficient automatic minutiae extraction algorithms focus only on ridge endings and ridge bifurcations. Moreover, the fact that both these types are the most common ones, supports this solution. A ridge ending is elementary to identify, it simply represents the extremity of the followed ridge (if it exists). For the ridge bifurcation, an intersection point with only one other ridge is needed (an intersection with 2 other ridges is a trifurcation), along with complementary orientation information.

The best solution for minutia's types recognition may be to combine the ridge following method and the structural pattern recognition approach. Ridge following would be used to detect a minutia point with any ridge termination, or intersection with another ridge. The structural method would provide the further analysis needed to more specifically identify the point (a ridge intersection, may be a bifurcation, a bridge, or a spur).

Mathematical Representations

Mathematical representations can be either formulas, as arrangements of different measures taken on the features, or geometric data, giving information on the position and the localization of the features' elements. The data are compiled in binary information. The analysis is thus elementary when knowing the coding rules. Usually, mathematical representations are assigned to the face and to the hand geometry traits. In theses cases, as previously explained, the issue is not to choose between several regions the best one, this selection has already been done and is fixed for every input of the same characteristic. However, as discussed later, the computation of the EVAL() function for these two traits, is still required. By knowing the stream's format (entered by the developer of the system) the function can easily analyze the values corresponding to each element or each measurement.

Internal Bits Codes

These internal codes are particular and different for each system. They are commonly used for coding the iris pattern. The analysis of such codes - for the matching, as there is no selection of meaningful areas within the iris - is based (in the case of the IrisCode) on logical operators and mathematical transformations that compute the degree of disagreement, between the input and the template. The codes will not be decomposed to analyze the meaning of each bit or groups of bits, unlike the bit strings of a mathematical formula. They are just compared one to another.

Now that the examination techniques have been presented, the applicable criteria for the EVAL() function are discussed herein below.

5.1.3.2 The Criteria for evaluating the regions' relevance

If the most relevant regions are chosen, it is only for accelerating the matching process, but while still ensuring a highly reliable result of the authentication operation. This is the reason why systems try to focus on smaller but really meaningful areas. What does "meaningful areas" means? It means regions that are easily differentiable from the other feature's regions and unequivocally recognizable among a substantial list of templates. The elected areas should exhibit (when possible) a "touch of originality". Two cases can provide this originality note:

- The unequal repartition of the information over the feature, or
- The presence of peculiar aspects on the feature

When this latest criterion is chosen, then not only it allows the reduction of the zone to analyze, but moreover, it permits the threshold's adaptation, before matching this area with a template. This threshold's modification is discussed in detail in the next section.

The aim of this subsection is to find efficient criteria, to locate within the whole biometric trait, the regions exposing the richest information for the matching with the templates. According to the traits, the concept of information "richness" changes. As already mentioned, the biometric characteristics can be separated in several groups, three in total. The first group gathers the fingerprints, the hand vein and the retina, traits for which the pattern is of a single type (minutiae, blood vessels). The second group contains the iris. Finally, the third group is composed of traits like the face and the hand geometry. The characteristics' patterns of those two last sets are assortments of various disparate elements. For instance, the face's pattern consists of the assemblage of the nose, the mouth and both eyes (at least). Each of these elements is completely distinct from the others.

In the first group, as all elements are of the same class, but not identical, finding peculiar ones is the solution for focusing on the most valuable zones. Concerning the second group (iris), a restriction on a particular area is not really fitting, because the elements taken individually are not necessarily representative of the input tested. Theoretically an extremely uncommon configuration, located on a certain part of the pattern, could be reported as an exceptional case and then extracted for the matching. However, in practice it's improbable, still because of the high level of details in the pattern and thus the quasi impossibility of knowing that an arrangement is scarce. Therefore, the whole feature is checked. As regards to the last set (face and hand geometry), the patterns of these traits present similarities with the traits' patterns of the first two groups. The features making up the pattern are dissimilar elements (as in the second group), but a selection between them is performed (most meaningful elements, as in the first group). For instance, the fact of collecting the eyes, the mouth and the nose for identifying a face, indeed corresponds to a (disguised) choosing of the face's most pertinent zones, as well as, the measurements of certain parts of the hand. However, the selections are invariant, they always pick the same elements (same G), thus, the EVAL() function will only estimate the degree of peculiarity (if any) for the characteristics of this third group. This is obligatory for a possible threshold's adaptation, matter of the whole research.

Consequently, for every group, there exists a particular way and a special reason, of computing EVAL(G). As a matter of fact, only the first and the third groups are concerned. As for the second group's traits, neither the location of a smaller region is performed, nor the search for exceptional features.

It is the study of the way of identifying a pattern that will help find the suitable criteria for appraising this pattern.

Every instantiation of a biometric pattern (a minutia point, a face element, a hand property measurement, etc.) can be expressed as a tuple, indicating all the properties’ values of the element: <**Feature**, **Type**, **Localization or Measurement, Relationships with other elements**>.

- Feature: the pattern used
- Type: the type (or weight) when applicable, the element’s name otherwise.
- Localization: it can be either the coordinates of the point (X,Y) according to the image orientation, or a measurement value.
- Relationships: this list is facultative. It is built for certain elements, for which the relations with the other elements are primordial (ex: the face elements, as shown later in this section).

Examples:

- A Minutia point: <Minutia Point, 1.91, (15, 28)> (The weight is used in replacement of the type’s name, because it is more explicit).
- A Face element: <Face Element, Nose, (62, 70), {LE, RE, M} > The list indicates the position of the nose, with respect to the eyes (LE: left eye, RE: right eye) and to the mouth (M).
- A Hand measurement <Hand Geometry, Hand’s Length, 7’’>

These properties allow the unequivocal identification of the element in the feature.

Some properties are more “discriminating” than others, depending on the feature and on the purpose of the EVAL() computation. For instance, the minutia’s type is the best criterion for locating the most relevant zones, in a minutia-based system, because its localization and its measurement are not significant properties. Minutiae don’t have predetermined spots on the fingerprints and as points, they don’t have either, a specific size to respect. On the other hand, the localization and the relationships between the elements are more meaningful for detecting any exception on a face.

As demonstrated at the beginning of the subsection, there are two possible criteria for EVAL(): the irregularity of the elements’ distribution on the feature (density) and the appearance of unusual features. This last criterion is the one that is related to the tuple defined for the pattern, since each attribute of the tuple, may “manifest” uncommon values.

Density of the feature on the characteristic

The density evaluation can be selected as a valid criterion for the appraisal of pertinent regions, in the image. However, only for the first group's characteristics. How is this density expressed in the images? In fingerprint images, it is the number of minutia points per unit area (square millimeter, for instance). For the vascular pattern, it will be the number of blood vessels per unit area also.

A grid of square one millimeter cells can be placed over the images and the minutia points within each cell will be counted. Then the average density can be computed, as a threshold. The cells with a density greater than that threshold will be considered as potential *Gs*. As this method can lead to an unmanageable number of *Gs*, due to the small unit area, gathering of adjacent cells is more appropriate. The algorithm can even start taking into account the *Gs*, only from a given size. For minutiae, twelve matched points, is the standard number for a correct authentication. Thus, considering the average density within one cell, it is possible to determine the average total number of cells that would expose twelve points.

<u>Example of the minutia points:</u>

Average Density per cell (Threshold) = 2 minutiae

Thus, the size of the *Gs* has to be equal or greater to 6 cells.

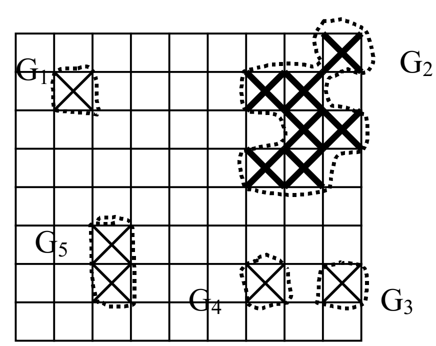


Figure 18: Selection of potential relevant regions

Figure 18, illustrates the grid laid on the pattern area. Each cell has an area of one square millimeter. The crossed cells are the cells displaying 2 minutiae or more (density greater or equal to the threshold). Five relevant zones, composed of adjacent crossed cells, are picked ($G_1,\dots,G_5$). Only one *G* (G_2) is elected in this example (more than 12 minutiae).

Conclusion: The density criterion has found one relevant region in the fingerprint's image, that the algorithm will then process for the matching with the template.

Remarks:

1. Both the input and the template images undergo the same analysis for the detection of relevant regions. Hence, by applying the same selection criterion (the density here), hopefully the same *Gs* will be detected in the input and the template of the same feature.
2. As stated earlier, the data are not anymore considered as pixels, because the feature extraction has already identified the minutia points on the image.
3. This example is also applicable to the vascular pattern.

Exceptions

The EVAL() function may also illustrate the exceptions in the characteristics. The recognition of unnatural element's types, measurements or localizations, can be reported as particular values for EVAL(). What would be the unit of measure then? It depends on the pattern's property, for which the value is particular:

- Element's *Type*: The notion of weight, reflecting the occurrence probability ($w_i = -\log_{10} p_i$), as in the minutia pattern case, can be applied to the EVAL() function. The algorithm presented in the Minutia's type section, works during the matching process and thus implies the presence of the template image. Here, there is no template involved yet, the issue is to find a *G*, within the whole feature. However, the algorithm here could use the weight property, to look for the rarest minutia's type in *F*. If found, then *G* will be composed of this rare point plus several others in its surroundings. The number of additional points relies on the size of *G*. This criterion is only applicable to patterns such as the minutiae or the vascular pattern, which exhibit the same basic elements, but with different shapes.

- Element's *Measurement*: These measurements can represent the length, the width, the element's size in a more general way. For a better reliability of the system, several measurements can be taken and averaged [66]. For each property (length, width, thickness, etc.), a range of "correct" values will be defined. When a value does not fit in this interval, it means that an exceptional element has been detected. The value for EVAL() will then be an arrangement of all the differences between the peculiar and the correct values, detected in the entire G. The correct values can be the intervals' boundaries. This "global" difference can be normalized. As a consequence, each potential G will indicate (with EVAL()) the proportion of rare elements it contains.

  Example of the Hand trait:

  The biometric trait that best portrays the use of this property is the hand (geometry).

  Properties measured:

  - **Length**: $X_0 \leq x \leq X_N$ (X_0 and X_N symbolize the "correct" boundaries for the length variable)
  - **Width**: $Y_0 \leq y \leq Y_N$ (Y_0 and Y_N symbolize the "correct" boundaries for the width variable)
  - **Thickness**: $Z_0 \leq z \leq Z_N$ (Z_0 and Z_N symbolize the "correct" boundaries for the thickness variable)

  Detection of an exception:

  if $(x < X_0)$ **then**
  $dx = |x - X_0|$
  else
  if $(x > X_N)$ **then**
  $dx = |x - X_N|$
  endif
  endif
  Idem for y and z

Function EVAL(G)

EVAL(G) = dx + dy + dz

EVAL(G) is built as a mathematical formula, with three types of variables (X, Y and Z). As a matter of fact, these variables rather represent unit of measures. They indicate the corresponding property of each distance value. As EVAL(G) is a global value for the whole *G*, another variable has to be introduced, for the mathematical formula. The formula (F) is essential to quickly identify the properties for which the divergences are worthwhile.

F = dx X + dy Y + dz Z

Selection of the best *G*

The *G* corresponding to the higher EVAL(G) is picked, the formula F is analyzed and the special property value will be exploited later, during the matching stage.

- Element's *Localization*: A large deviation in the coordinates of an element, by comparison to a general accepted model, could authorize the threshold's modification. The EVAL() function could then measure the deviation degree of the element regarding the normal model. When the data are geometric data, then measures of angles will be appropriate. This scheme is presumable only if the normal locations of the elements are predefined.

  Example of the face trait:

  This property is especially suited to a face-based system. The face's elements are recognized to have relatively known positions, ones with respect to the others. Their geometric representations help detecting the "bizarre" cases. Even if, the probability of having on the face, an element encountered far from its ordinary position, is particularly low.

  Measurements:

  They are the coordinates of the elements, ones with respect to the others. The elements chosen are the eyes, the nose and the mouth.

Each element will then stand alternately, for the reference system. The general model is represented in terms of range of acceptable coordinates for each element. The correct model should be based on the elements' coordinates of a theoretically "perfect" face (with a perfect symmetry with regard to the median line). The margins of variations will then come from analysis of real faces. They can be averaged from a large database of face representations. Each element (either in the correct model or in the inputs) will then have three coordinates. For one face, twelve measures will be reported. When considering Figure 19, the ranges of correct values (in terms of angle measures), with respect to the nose (tip), are:

RE: Right Eye	$40° \leq RE \leq 85°$
LE: Left Eye	$95° \leq LE \leq 140°$
M: Mouth	$225° \leq M \leq 315°$

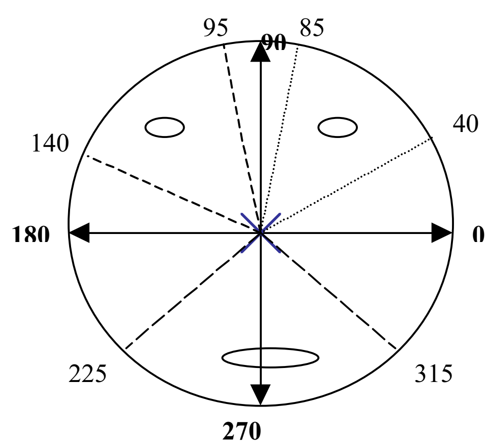


Figure 19: Correct Model (Coordinates of the elements, with the nose as the reference)

These three elements are not points, but rather figures. Here to simplify, it will just be assumed that, the element's left end must have an angle greater than (or equal to) the minimum value and the right end angle should be inferior (or equal) to the maximum angle specified. Hence for each element, the ends' angles will be compared to these boundaries. When, one of the coordinates does not meet the condition, then, the difference between this angle and its closest boundary is computed, like in the "Element's Measurement" subsection, just above.

Figure 20 shows the situation where the left eye is the reference.

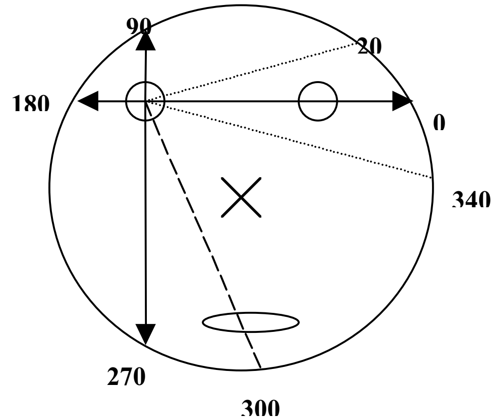


Figure 20: Correct Model (the left eye is the reference)

Detection of an exception:

The algorithm is the same as the one in the previous subsection. As there are four references, the coordinates for each element are noted as a set of four values (for more simplicity):

$LE(d_{LE}, d_{RE}, d_N, d_M)$

$RE(d_{LE}, d_{RE}, d_N, d_M)$

$M(d_{LE}, d_{RE}, d_N, d_M)$

$N(d_{LE}, d_{RE}, d_N, d_M)$

Each d_{xx} is the absolute value of the difference between the angles of the element (left and right ends) and the normal angles for this element.

Function EVAL(G):

EVAL(G) will again be the sum of the differences, which are absolute values.

$EVAL(G) = \Sigma d_{LE} + \Sigma d_{RE} + \Sigma d_N + \Sigma d_M$

Selection of *G*:

With each *G* area, will be associated the coordinates of the four elements and the value of EVAL(), for the *G*'s selection.

- Element's *Number*: This property is akin to the previous one, in the sense that the "correct" number for each element has to be known prior the authentication. Any discrepancy would be reported and noted as a normalized estimation of the divergence. Still, here again, the applications of such a procedure are quite scarce.

When EVAL() estimates the degree of exception carried by a pattern, then it directly indicates the possibility of adapting the threshold. The higher the value of EVAL() will be (assuming that this value changes in the same direction than the level of peculiarity), the higher the chances for adjusting the threshold.

What happens when no particular G is found with EVAL()? (when neither the exception criterion, nor the density one has revealed a particular area) Then the whole feature is compared, because a small part of it wouldn't be reliable.

Once the evaluation of the potential *Gs* has been done (according to EVAL()) and that one of them has been elected for representing the whole feature, then at this point, the decision of modifying or not the threshold can be taken.

5.1.4 Threshold

After having selected the best *G*, what argues in favor of a threshold's adjustment? The standard for the threshold's adaptability is generally, the presence of a factor of singularity. Yet, as shown with the level of security, it can also be induced on purpose, to fit particular conditions. The connection between the factor of singularity and the EVAL() function, exists only when EVAL() symbolizes the exceptions on the patterns. For the other notion of EVAL(), the density of the feature, it exists only to save time during the authentication process, by revealing the parts that expose enough data for an accurate identification. If these data don't carry any noticeable properties, then the issue of a threshold's alteration is not tackled. Therefore, the function should always mention the level of rarity exhibited by the corresponding *G*. In this perspective, the use of EVAL() will be twofold: to inform on the possible singular situations, and to indicate the most relevant areas of the feature, for the matching. The function will then be a set of two elements (estimation of the peculiarity's degree and evaluation of the region's density), which natures will change according to the feature and the data representation, as explained in the previous section. Both criteria will probably designate different critical zones in the feature. Yet, the exception degree is first consider, as it has more impact on the authentication process (definition of a meaningful zone within the feature and modification of the threshold hopefully).

The decision of modifying a threshold, as well as the definition of its new values, are not improvised resolutions. As the authentication is a machine process, all the possibilities have to be thought of, at the system design. The machine can't take decisions by itself when it has never experienced the situation before. Except maybe if one extrapolates and considers the addition of artificial intelligence software, with a methodology similar to the one behind artificial neural networks[10]. Then the system could learn from past situations, how to deal with equivalent ones. This aspect will not be discussed in the present thesis, rather in this section the focus is on the necessity to conceive a general logic for the threshold's modification. This general logic should work even when the "unusual" conditions occur. The concept to be understood is that the algorithms, when conceived**, should anticipate and integrate** the prospect of threshold's adjustment.

The algorithm developed for the minutia's type criterion, was a good example of the idea of a global solution, adaptable to both the common and the

---

[10] Free Online Dictionary Of Computing: *"(ANN, commonly just "neural network" or "neural net") A network of many very simple processors ("units" or "neurons"), each possibly having a (small amount of) local memory. A neural network is a processing device, either an algorithm, or actual hardware, whose design was inspired by the design and functioning of animal brains and components thereof. Most neural networks have some sort of "training" rule whereby the weights of connections are adjusted on the basis of presented patterns. In other words, neural networks "learn" from examples, just like children learn to recognize dogs from examples of dogs, and exhibit some structural capability for generalization."*

uncommon cases of identification. Indeed, the procedure always operates in the same manner. This way of proceeding was permitted by the “universality” of the type property. Every minutia has a certain type, therefore the fact of processing it, is a general operation that does not correspond to any particular behavior. The singularity of the configurations wasn’t in fact, really “noticed” by the algorithm (at least during the process). The combinations for a correct identification were infinite, and the algorithm only “knew” the final authoritative value. At the end, it happened that some of the configurations were only composed of a very few points, due to their types’ peculiarity. As a result, the uncommon cases did lead to an acceleration of the matching process, by decreasing the total number of compared minutiae, which was the threshold.

The Fuzzy Logic solution would be closer to the artificial intelligence logic, in the definition of the set of rules. All possibilities are exposed and for each of them, an action or value for a particular variable is defined. The only issue is to determine the rule corresponding to the actual input to test. In this method, the exceptional cases are explicitly expressed among the system’s list of rules. Even if the fuzzy logic is a methodology inspired by human reasoning, it is efficiently implemented in both hardware and software, without any human interference. Hence, the algorithm is able to select the suitable rules for any special case, (provided it has been foreseen), as this decision rests on precise variables’ values. Maybe it is not unnecessary to point out an aspect of the use of the fuzzy logic, especially in the example of the level of security. It could seem that the concept of exception had been handled quite differently with the level of security criterion. The special situations there, occurred when the administrator chose to change the degree of security, from the normal level, to either the high or low one. The cases appeared to be reversed, compared to the usual situations where, the algorithm analyses the feature and detects an uncommon aspect. Here the result of the procedure (the presence of a peculiarity) becomes a goal to reach by the system. Still, the outcome regarding the modification of the algorithm, is the same. It is the fuzzy rules that cause directly the threshold’s adjustment.

Those two methods are well adapted to the two circumstances that can occur prior to a threshold’s modification. Namely, the case where the exceptions are bounded or predictable at least (fuzzy logic), and the one where on the contrary, the “anomalies” (or their combinations) are infinite (method of the “rarity weight”). In this later solution, the uncommon situations don’t benefit from a definite, special treatment. Nonetheless, by having integrating the understanding of flexible threshold, the systems succeed in taking advantage of the particular cases.

Once the resolution to change the threshold value has been taken, the next issue is to set the new threshold. The level of particularity revealed by the EVAL() function, defines this new value, depending on the methods used by the systems.

This eventual threshold’s adjustment closes the definition of this generic procedure, hopefully adaptable to any biometric characteristic. The following section sums up the whole process using a diagram.

5.1.5 The Procedure’s Schematization

A scheme of the procedure is useful to summarize the different steps leading to a possible threshold’s modification (Figure 21).

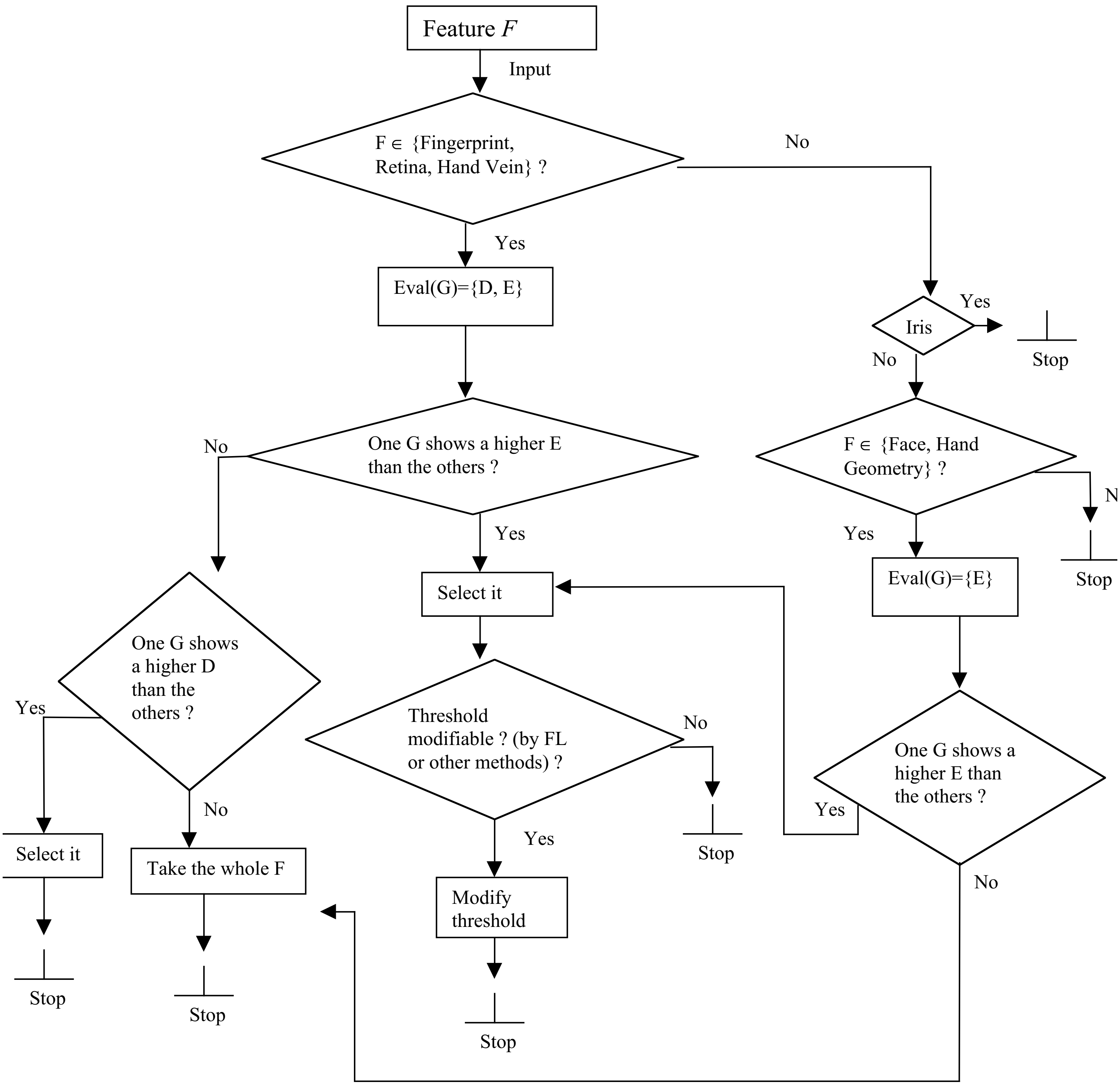


Figure 21: Generic Procedure diagram

The whole feature *F* is submitted to the system as the starting input.

- If *F* is part of the first group of biometric features (fingerprint, retina and hand vein), then, the EVAL() function is a pair of two criteria, the density (D) and the exception (E): EVAL(G) = {D, E}. For selecting the best *G*, the exception criterion prevails over the density, therefore the elected *G* will have the highest exception degree. The threshold's adaptability is then checked, with methods like the Fuzzy Logic, or others. If the requirements are met then, the threshold is changed, otherwise it is kept as it was initially. If it happens that none of the *Gs* contains uncommon elements (or all present identical value for E), then the density criterion is considered at this point. The same logic is used: find the *G* with the highest density, or choose any of the potential *Gs*, when the density is equivalent for all of them.
- When the feature is the iris, the only member of the second group, then the algorithm stops, because the EVAL() function is not computed for this feature.
- For the third group of features (face and hand geometry), it indicates only the exception degree, as the density notion is not valid for these traits. If one *G* exhibits a higher value for E, then it is elected, otherwise, any of them is chosen.

The procedure ends with a particular region of the feature selected, for the further matching.

The last section raises an issue related to the matching stage, succeeding the possible threshold's modification.

5.2 A Further Consideration

The procedure did not make any allusion to the matching step. It was more concerned with the feature alone and its handling, as well as with the reasons that would cause the threshold's adaptation. This matching stage is of course completely related to the threshold. However, there was no precise reason to make a distinction between the templates and the inputs, at this level. The objective was to show how a given feature could lead to a threshold's modification, whatever its classification. Now that this has been accomplished, the matching stage can be considered.

All the reasoning was done, assuming the input and the template exhibit the same data format. What if, for a reason or another, the matching has to be done between different representation types of the same biometric trait? One could imagine the situation where, international police services would like to cooperate, by exchanging criminals' identification information. The same biometric characteristic can be represented in various ways, as illustrated previously. For data originated from a system A, to be read and processed by a system B, it is necessary to transform these data, for system B to be able to process them. The obvious obstacle in implementing this stage is the several versions it can have. There should exist a conversion device, for every possible pair of different data representations, existing among the biometrics systems. Moreover, this should be done for every biometric trait used in authentication. The "alien" data would necessarily have to be transformed in the local representation, as all the templates have this local format.

The ultimate, but radical solution would be to agree on a standard model of representation, for each group of features. This way, it would solve this issue of data exchange among systems. It is a radical solution, because it would force all the systems' redesign. Furthermore, the biometric authentication business hasn't reached this point yet. For now, the priority is to succeed in popularizing the application of biometrics for identification. This process of popularization tries to reorient the utilization of this kind of authentication, from the forensic domain, (or high-security areas control) to common life access control. From this viewpoint, there is no need for data exchange. Not for now, but this is inevitably another type of consideration, that sooner or later will have to be resolved. Indeed, it is clear that in a near future, given the proliferation of biometric devices, the need of connecting them will impose itself.

Summary and Transition

Despite the differences among the biometric characteristics, their processings follow globally, the same strategy. The way of evaluating them, selecting the areas worth comparing with the templates, appraising the degree of scarcity revealed by the features, is quite alike whatever the trait. The distinction is in fact more significant at the data’s format level, as various biometric features can be coded in the same ways (mathematical data, digital information, etc.).

Chapter 6: Simulations/Implementations

This last chapter presents the implementation of a part of the generic algorithm, depicted in the last diagram (Figure 21). The implementation concerns only the fingerprints, but the whole process is executed. The goal is to localize, within an input of the entire feature *F*, the most representative part of it, *G*.
The JAVA language was used for the coding.

6.1 The concept

The input *F* is not an image, as in most of the AFIS. Rather, the minutia points are directly entered as points, with their attributes. Each minutia is a tuple of the following structure: <*Minutia_number, Type, Direction, X-value, Y-value, Weight*>.
The *Type* and the *Weight* attributes have exactly the same meaning however, the *Type* is used in a concern of simplicity for the user, when viewing the set of minutiae and the *Weight* property is employed for the computation of the subsets' relevance. *Weight* = -log p_i (with p_i being the occurrence probability of the type). The *Direction* is useful during the matching stage. The *X-value* and *Y-value* are the coordinates of the points, on a two-dimensional plan.
The user enters on the command line, the maximum values for the Type, the Direction, the X and Y values, as well as, the number of points in the set.
Ex: *java file_name 10 8 80 24 36*
This command means that there are 10 types of minutiae, 8 directions possible for a point, it sets the coordinates system (80 as the maximum abscissa and 24 as the maximum value on the Y-axis) and indicates the total number of minutiae in the input *F*. It also asks the user for the occurrence probabilities. The set of minutiae is generated, following the probabilities of occurrences of the different types. Each minutia is assigned its attributes.

The *Gs* subsets are formed from the input set, following the exception type criterion. The size of the *Gs* is set to 18 points, at most. This decision is rather arbitrary. Given the 12 matched points standard, it seems reasonable, to have subsets of 18 points, for the comparison. In a first step, all the rarest points are detected (the ones with the highest weight). Then, for each of them, their neighbors are added to the corresponding sets, as long as the total sum of the points' weights doesn't reach the threshold sum. This threshold sum is the sum of the weights of 18 minutiae of the most common type. This logic resembles the one depicted in the Chapter 4, about the minutia's types. Therefore, in each subset, there will be one of the rarest points and 17 or less, of its closest neighbors.

As the probabilities of appearance are entered by the users, it can happen that all the probabilities are equal. In this case, the result of the algorithm will be the entire set, entered as the input. As no point is exceptional, it is safer to compare the whole set.

The density criterion is not used, because as the input is a set of points and no longer an image, the notion of selecting a smaller but denser part of it, doesn't make sense anymore. The size of *G* is no longer considered in terms of area, but in terms of cardinality. Moreover, this cardinality has a maximum number, thus a denser area, will mean a subset with a higher cardinality, which does not bring any benefit to the matching stage. Originally, the improvement that this criterion should bring, is the reduction of the size of the image to compare. With a set of points, it is an inapplicable parameter.

6.2 The Analysis

This section defines the entities involved in the algorithm, to further allow the determination of the classes.

The first object that is needed is the minutia. Both the input and the output are sets of minutiae, however the sets' structures are not identical. The input set is a simple array of minutiae (one-dimension), when the output, the *G* subset, is a fraction of a two-dimensional array, regrouping all the potential *Gs*. This two-dimensional array uses the input set to arrange the minutiae, regarding the exception type criterion. Each row in this intermediary representation is a potential *G*.

The following scheme shows the relations with the three entities:

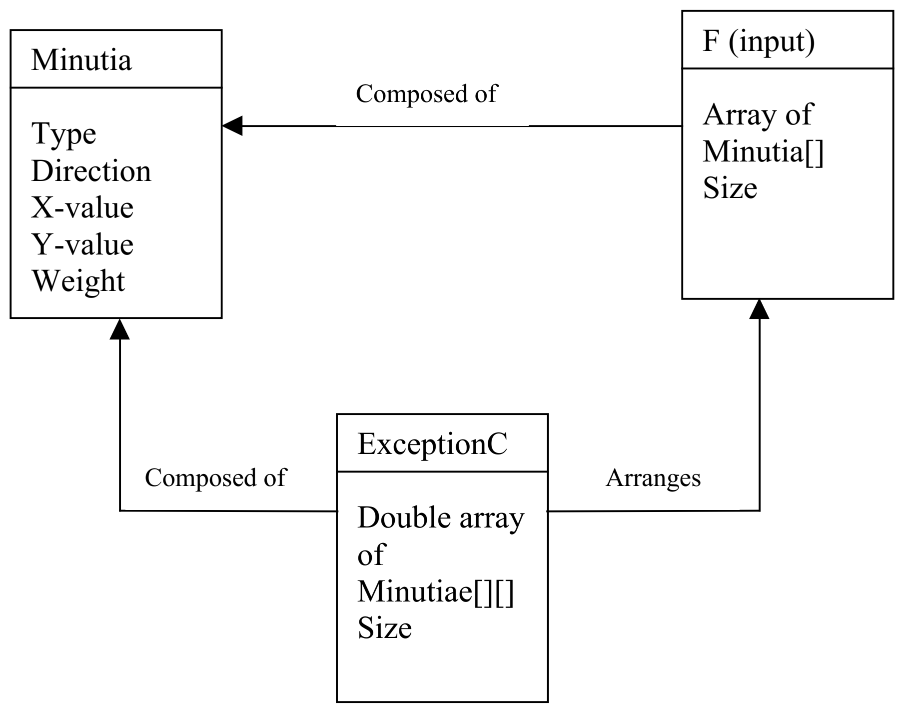


Figure 22: Entities and Relationships

6.3 The Implementation Details

Here follows the goal of each JAVA class developed for the algorithm. The purpose is to explain globally what each class does, without going into details.

6.3.1 The Generic Class (Main)

This class is the main class. It asks the user for the minutiae parameters (the maximum values). Regarding the types' number specified by the user, an array of occurrence probabilities is built and filled by the user himself. It then creates an objet *TAB* that will contain the generated input minutiae. Then an *ExceptionC* object, containing the rarest points is built from the input set. The subsets of potential *Gs* are formed, from this input. If the number of rare points in the ExceptionC array is the same than the number of minutiae in the input array, it means that there is no rare point, all are equivalent, and therefore the result is the whole input. If only one rarest point exists in the whole input set, then its corresponding subset is displayed. Otherwise, from all the potential subsets, the best one is elected.

6.3.2 The Tab Class

A *Tab* object is a one-dimensional array of *Minutia* objects. The constructor of the Tab object uses all the data provided by the user to generate the different minutiae. Each occurrence probability in the probabilities' array is read and multiplied by the total number of points specified by the user. Whatever the probability values, the total number of points must be equal to the number given by the user. To satisfy this condition, the result of the multiplication (probability multiplied by number of points) is rounded to the upper integer. The minutiae are created (the properties are defined) during the process, and the Tab array is filled. As soon as, the total number is reached, the points' generation stops. This class contains also a second constructor that only defines the size of the *Tab* object, without filling it with minutiae yet. A method has been written for deleting a particular cell of the array, given its position in the array. Another one allows the cloning of a *Tab* object. This cloning method first uses the second constructor to build an empty Tab, then copies each element of the original object to the cloned one.

6.3.3 The Minutia Class

A Minutia object has 5 attributes: type, direction, X-value, Y-value and weight. The minutiae are generated "pseudo-randomly". The types have already been computed from the probabilities, when creating the Tab array. However, the other attributes still need to be determined. They are random values (except the weight that is computed from the occurrence probability), produced while regarding the maximum number indicated in the command line for each property. The Counter method of the Minutia class generates a random number. It then takes the absolute value of this random number, modulo the user's input. This modulo is necessary to avoid numbers greater than the one given.

6.3.4 The ExceptionC Class

An *ExceptionC* object is a two-dimensional array that goes through the *Tab* array of input minutiae and extracts the ones with the highest types. These points are placed on the first column of the two-dimensional array. The constructor of this class first goes through the entire Tab array once, to find the maximum weight. Then a second time to count the elements exposing this maximum weight and copy them in an array. The size of the ExceptionC array is then known, for one dimension at least (the number of rare points). The other dimension is fixed to 18 (the neighbors). The array is then of equal size in its width, for making its exploration simpler, even if, for some points less than 17 neighbors may be collected. The temporary array, containing the rare points, is copied in the first column of the ExceptionC array.

To build the subsets of potential *Gs*, each point of the first column is considered. Its coordinates are used to compute the Euclidean distance with each minutia of the input set. The formula for computing the distance between two points *a* and *b* is: $\sqrt{[(x_a-x_b)^2 + (y_a-y_b)^2]}$. The method that constructs the subsets fills each row (one row corresponds to a subset) with the points that have the smallest distances to the "head point" of the row (the rarest one), excluding distances equal to 0 (same point). For each rare point, the entire Tab array is analyzed, to find the closest point. This point is added to the row and deleted from the Tab array. While doing so, the sum of the added points' weights is computed and compared at each addition, to the threshold sum. This threshold sum is equal to 18 times probability of the most common type. It has been computed with the first element of the probabilities' array, in the main procedure. As soon as this one is reached or exceeded, or that 17 neighbors have been found, then the subset is considered to be complete. Before the constitution of each subset, the Tab array is reinitialized (use of the clone method written in the Tab class). The next method is for selecting the best subset, the one with the lowest number of points or the highest weights' sum when all the subsets' cardinalities are identical (it may happen that two or more sets present the same cardinality, but with distinct weights' sum, both exceeding the threshold). This method returns the cardinality of the smallest subset (the one containing the "heavier" points) and indicates its index in the *ExceptionC* array.

This simple implementation illustrates how easy it is to select a particular set of meaningful points, for the matching with a fingerprint template.

Conclusion

The security gaps are still large in open networks of all kinds, whether it is the Internet or the network of cellular telephony. As explained before, a secure authentication operation is a key element in the process of filling these weaknesses.

The automatic authentication systems lay on different concepts, different types of data, different ways of processing these data. However, all aim to provide accurate results in the most convenient manner possible, for the user. The achievements vary from a system to another.

The benefits automatic authentication systems would gain from the adaptation of the acceptance threshold are obvious, even before studying the possibilities in details. As its qualifying indicates, a flexible threshold should adapt itself to any situation (a priori), widening its scope of applications.

Concerning Automatic Fingerprint Identification Systems, many diverse parameters appeared, at first sight, to be valid criteria for the threshold's modification, whether it is at the features' level, the application's or the equipment's one. The main condition to satisfy, to be elected as a valid criterion, is to not weaken the overall performance of the system (its reliability), while bringing an improvement in the matching stage. This improvement can either be the reduction of the operation time, or the simplification of the process. Most of the time, both notions are linked. Moreover, the new values should be chosen in such a way that they would balance the False Acceptance Rates and the False Rejection Rates.

Only two parameters succeeded in fulfilling the requirements: the minutia's type criterion and the level of security chosen by the administrator. To really appraise the validity of such decisions, computation techniques were defined and adapt to each parameter. The Fuzzy Logic was found completely suited to the level of security criterion. Indeed, this criterion is already used in many existing AFIS, to regulate the threshold regarding the several False Acceptance rates available to the users.

Regarding the minutia's type criterion, a method based on the occurrence probabilities of the miscellaneous types was proposed, to reduce the required number of matched points in the presence of uncommon minutiae.

In an objective of generalization and resolution of the problem from a higher level, a generic procedure was detailed, to demonstrate how to get to the decision of modifying the threshold, given the feature at the beginning of the authentication procedure. This procedure has been conceived as general as possible, not limited to any feature or data representation in particular. It can therefore be implemented, hopefully, to a large number of biometric authentication systems.

This thesis has established and illustrated the adaptability of acceptance thresholds in fingerprint authentication methods. The exploitation of such a property is nothing but rewarding for the performance of the systems. A more reliable, user friendly and faster system for authentication, is the perfect match for the electronic commerce and the cellular world.

References

[1] Computer Industry Almanac Inc. « Over 147 Million Internet Users Worldwide at Year-end 1998 » (1999):
http://www.c-i-a.com/199902iu.htm

[2] SET Secure Electronic Transaction Specification. Book 1 : Business Description Version 1.0 May 31, 1997

[3] "Cellular Phone Fraud" by Dana Roettger (1998):
http://www.csm.ohiou.edu/comt391w/droettger/comt391.html

[4] Keytel. « Cellular Phone Fraud » (1997):
http://www.keytel.com/cell.htm

[5] « Overview of secure electronic payment systems » :
http://mba.vanderbilt.edu/student/mba98/jeffrey.nuckols/secure_online_payment/overview.html
(Computer Money : A Systematic Overview of Electronic Payment Systems, Andreas Furche and Graham Wrightson, dpunkt : Heidelberg, 1996)

[6] "CyberCoin: Micropayments Service Overview":
http://www.cybercash.com/cybercash/services/cybercoin4.html

[7] "Electronic Payments With eCash":
http://www.digicash.com/index_e.html

[8] « How Mondex works?" (1998):
http://www.mondexusa.com/html/content/technolo/technolo.htm

[9] "Transaction Net: Payment Methods Online and Off" (1997):
http://www.transaction.net/payment/index.html

[10] Open Market Home We are Internet Commerce:
http://www.openmarket.com/

[11] Netmarket Name Brands at Warehouse Prices:
http://www.netmarket.com/

[12] CyberCash, Inc, Home (1998):
http://www.cybercash.com/cybercash/

[13] “What is Echeck? » (1998):
http://www.echeck.org/kitprint/audio_conference.html

[14] EE 4984 telecommunication Networks Project 1. Cellular telephone Fraud, by Kimberly A. Stewart (1995):
http://fiddle.ee.vt.edu/courses/ee4984/proj_95/stewart.html

[15] Introduction to Authentication (1998):
http://www.nacn.com/products/wireless/authcenter.html

[16] USC/ISI Technical report number ISI/RS-94-399. « *Kerberos: An Authentication Service for Computer Networks* » by B. Clifford Neuman and Theodore Ts'o :
http://nii.isi.edu/publications/kerberos-neuman-tso.html

[17] “*bsy's Explanation of Zero Knowledge Proofs*”
http://www.cse.ucsd.edu/users/bsy/ZKP.html

[18] Identification and Authentication. NIST Computer Security Handbook (1997).
http://bilbo.isu.edu/security/isl/hk_i&a.html

[19] “*Biometric Authentication*” by Jared McDonald, B.C at University of Otago, New Zealand, 1994:
http://spook.otago.ac.nz:800/members/jared/research/honors/

[20] « *About Fingerprints* » BPI Biometric Partners Inc (1999):
http://biometricpartners.com/Finger_Prints/finger_prints.html

[21] « *Forensic Science Web Pages*. *Personal Identification. Fingerprints* » (1997):
http://users.aol.com/murrk/page6.htm

[22] “*An Identity-Authentication System Using Fingerprints*” by A. Jain, L. Hong, S. Pankanti and R. Bolle. Proc. IEEE, Vol. 85, No. 9, pp. 1365-1388, 1997.

[23] Digital Persona : “*About the fingerprint*” (1998):
http://www.digitalpersona.com/afprint/html/body_fbasics.html

[24] FBI Educational Internet Publication : « *Fingerprint Identification* » (1997):
http://www.fbi.gov/kids/finger/fingerpt.htm

[25] « *Detecting Fingerprint Singular Points by a Hierarchical Model* » (1997):
http://object.njit.edu:2000/~austin/research/paper/p4.html

[26] LawSearch. « *Pattern Types* » (1999):
http://www.chickasaw.com/~waedens/fpc/types.htm

[27] « *A Fingerprint Classification Technique Using Directional Images* » by M. Ballan, F. A. Sakarya and B. L. Evans. 1997 IEEE Asilomar Conference on Signals, Systems, and Computers : http://www.ece.utexas.edu/~bevans/papers/1997/fingerprints/index.html

[28] "*Development of a Mathematical Formula for the Calculation of Fingerprint Probabilities Based on Individual Characteristics*" by J. W. Osterburg, T. Parthasarathy, T. E. S. Raghavan and S. L. Sclove. Journal American Statistic Association, 72, 772-778, 1977.

[29] "*The science of Fingerprint Identification Lesson one 'Ridges'*" (1996): http://www.brawleyonline.com/consult/fp1.htm

[30] "*Computer-vision-based approach to personal identification using finger crease pattern*" by D. G. Yoshi, Y. V. Rao, S. Kar, V. Kumar and R. Kumar. Pattern Recognition. Vol 31. No. 1 pp15-22, 1998

[31] "*An Approach to Fingerprint Identification by Using the Attributes of Feature Lines of Fingerprint*" by X. Qinghan and B. Zhaoqi. Conf: Int. Conf. (8th) on Pattern Recognition (Paris, France October 27-31, 1986), IEEE Publ. 86CH2342-4, 663-665.

[32] "*Finger Image Identification Method for Personal Verification*" by M. Takeda, S. Uchida, K. Hiramatsu and T. Matsunami. Conf: Int. Conf. (10th) on Pattern Recognition, 1990.

[33] "*Computer Vision and Image Processing: A practical approach using CVIPtools*" by Scott E. Umbaugh. Prentice Hall PTR, 1998

[34] "*An Approach to Fingerprint Filter Design*" by L. O'Gorman and J. V. Nickerson. Pattern Recognition, Vol. 22, no. 1, 1989, 29-38.

[35] "*Fingerprint Image Enhancement : Algorithm and Performance Eval*uation" by L. Hong, Y. Wan and A. K. Jain. IEEE Transactions on PAMI, Vol. 20, No. 8, pp.777-789, August 1998.

[36] Fingerprints - Search and Match Algorithms / Systems AFIS (1998): http://www.east-shore.com/tech.html

[37] "*Direct Gray-Scale Minutiae Detection in Fingerprint*" by D. Maio, and D. Maltoni. Tech. Report n. 105, CIOC-CNR, Universita' degli studi di Bologna, Sept. 1995.

[38] "*Fingerprint Identification Using Graph Matching*" by D. K. Isenor and S. G. Zaky. Pattern Recognition, Vol. 19, 1986, 113-112.

[39] « *Point Matching Algorithm* » (1998):
http://www.cse.msu.edu/~dutanico/Fp/match3.html

[40] IriScan. The Scientific Basis for Iris Recognition, by John Daugman:
http://www.iriscan.com/basis.htm

[41] ID3D HandKey Product Brochure, Recognition Systems, Inc. Received 1994.

[42] "*Introduction to Personal Authentication*":
http://www.ecom.or.jp/about_wg/wg06/english/intro/abstract.htm

[43] Technology Recognition Systems. Facial Thermograms:
http://www.betac.com/threshold/facial.htm

[44] Network Computing Online "*Six Biometrics Devices Point The Finger At Security*":
http://www.networkcomputing.com/910/910r1side1.html

[45] Digital Persona "*Is U are U for you?*":
http://www.digitalpersona.com/html/isforu.html

[46] Sony Online World "*Products LineUp : Fingerprint Identification Unit*":
http://www.world.sony.com/Electronics/Components/Products/product57.html

[47] "*Mixing Biometrics and Integrating Circuit Technologies with Algorithmics. Fingerprinting on-chip and Security Smart Card for improving authentication to aid securing services delivery*" by D. Guinier. Conf: 10th Canadian Information Technology Security Symposium, 1998.

[48] American Biometric Company "*Biomouse*":
http://www.biomouse.com/products/biomouse.htm

[49] "*Biometrics Gold Cognitive Devices*", (1998):
http://innotts.co.uk/~joerice/

[50] Thomson-CSF : « *Cellular Phone Security* »:
http://www.tcs.thomson-csf.com/Us/fingerchip/Applications/appcellsec.htm

[51] "*An approach to fingerprint identification by using the attributes of feature lines of fingerprint*" X. Qinghan and B. Zhaoqi. Conf: Int. Conf. (8th) on Pattern Recognition (Paris, France October 27-31, 1986), IEEE Publ. 86CH2342-4, 663-665.

[52] LawSearch "*Points of Identification*" (1999):
http://www.chickasaw.com/~waedens/fpc/idpoints.htm

[53] « *Point Matching Algorithm* » (1998):
http://www.cse.msu.edu/~dutanico/Fp/match3.html

[54] "*Fingerprint Image Enhancement: Algorithm and Performance Evaluation*" by L. Hong, Y. Wan and A. K. Jain. IEEE Transactions on PAMI, Vol. 20, No. 8, pp.777-789, August 1998.

[55] BPI Biometric Partners Inc. (1999) "*About Fingerprints*":
http://biometricpartners.com/Finger_Prints/finger_prints.html

[56] Network Computing Online "*Six Biometrics Devices Point the Finger At Security*" (June 1998): http://www.networkcomputing.com/910/910r1.html

[57] "*Fuzzy Logic*" (1999):
http://www.attar.com/pages/fuzzy.htm

[58] "*Fuzzy Logic Tutorial*" by Steven D. Kaehler :
http://www.seattlerobotics.org/encoder/mar98/fuz/flindex.html

[59] Fuzzy Inference Development Environment (F.I.D.E) "*How does Fuzzy Logic Work?*" (1999):
http://www.aptronix.com/fide/howfuzzy.htm

[60] Veriprint 2100:
http://www.neutron.com.sg/BII.htm

[61] The Veriprint 2000:
http://www.clever.net/security/veri.html

[62] "*Fourier, fingerprinting technique promises new, low-cost discrimination*", An Interview with M. Fiddy, M. Testorf and J. Lin; University of Massachusetts/Lowel, by Frederick Su. OE Reports Nov. 1998.

[63] Visionics Corporation "FaceIt Technology Overview":
http://www.faceit.com/live/frameset.html

[64] Plettac Electronics. Access Control Systems:
http://www.plettac-electronics.com/zks/index.html

[65] "Face Recognition by Elastic Bunch Graph Matching" by Laurenz Wiskott, Jean-Marc Fellous, Norbert Krüger, and Christoph von der Malsburg:
http://www.cnl.salk.edu/~wiskott/Projects/EGMFaceRecognition.html

[66] Recognition Systems, Inc. "Hand Geometry Today" by Dick Zunkel:
http://www.recogsys.com/rsi_public_html/rsitech.html

[67] “Practical Computer Vision Using C” by J.R Parker. Wiley Professional Computing. 1994