# THE PERSONAL IDENTIFICATION NETWORK: BIOMETRIC SYSTEMS VIA THE INTERNET: PART I

*Lee Luan Ling, Miguel G. Lizarraga*

DECOM-FEEC-UNICAMP
Campinas, SP, Brasil
Email: lee@decom.fee.unicamp.br

## ABSTRACT

The use of the Internet as a means of accessing a large variety of network services requires the implementation of security procedures that ensure the authenticity of users. Currently most technology that relies on a personal identification number (PIN) or password for personal authentication purposes hardly meets the satisfactory security level. In this paper we present a personal identification system that offers personal identification services via the Internet based on personal biometrics characteristics (signatures, faces and fingerprints). The implemented personal identification system, named the Personal Identification Network, offers two basic real time services via the Internet: the visual consulting service and the automatic personal verification service. The prototype of the proposed personal identification system for handwritten signatures now is found implemented, operating and can be accessed via the *Web* site: http://www.lrprc.fee.unicamp.br/id. A detailed description of the implemented method for biometrics signature information processing and feature extraction, as well as the implemented decision algorithm for automatic signature verification, can be found in a parallel submitted paper (Part II).

## 1. INTRODUCTION

Since the end of the nineteenth century the technological progress in electronics and telecommunications has been significant. The evidence of this progress was revealed by the appearance of telegraph, telephone, radio, television, satellites, and most recently cellular telephone. By the end of the twentieth century and the beginning of the new millennium, the development and consolidation of the computer and communication network technologies have caused some profound transformations in every sector of our society. In particular, we can cite the Internet technology that no doubt has caused strong impacts in our daily lives.

Through the Internet the exchange of information and the utilization of network services, such as electronic mails, sending and receiving files, advertising, on-line conversation, commercial transaction, etc., seem much easier than ever. In fact, we are on a new era of information, where there is no more frontier of communication. On the other hand, on this new era of information, information has acquired its monetary value that has motivated a large variety of illegal activities practiced by hackers – who rob information for their own benefit. The damage resulted from such a kind of activities frequently can reach a significant magnitude to the legitimate owner when the stolen information is for some financial purposes at the legitimate one´s expense [1]. A typical example of such a kind of fraud is the case that hackers capture one's credit card information during transaction on computer networks and later act as the credit-card's legitimate owner.

Interesting enough nowadays, under the client/server operation principle adopted by most computer networks, the network server is capable of informing surely the account name/number, the organization and the country, and through which computer, subnet and network the user is connected. However, there is no way for the network server to identify the person who is using the computer to access the network service. In fact, offering protection to the network information, services and users via biometrics is widely desired but still moderate. Some pioneering work, which seeks solutions to this problem, has been reported [2,3,7,11]. In this paper, we describe a prototype of a biometrics system via the Internet, named the Personal Identification Network, which has the goal of illustrating the feasibility of offering personal identification services in real time through communication networks, and in particularly, via the Internet. In Section 2 we define our model of biometrics systems via the Internet. Section 3 is dedicated to the detailed description of the implementation of the Personal Identification Network. Finally Section 4 expresses our final conclusions and comments.

## 2. THE SYSTEM MODEL

The personal identification system via the Internet actually performs a two-fold identification: (1) identification of the service user, which in general consists in non-biometric identification, and (2) biometric identification. For the first type of identification, one of the important features of the proposed prototype is that geographically dispersed users can access the biometric service independently, simultaneously and remotely. Under such a quality or requirement the biometric system should also be able to offer different non-biometric methods of identification for each subject. An example of this situation is that one's social security number and driver license number may be requested separately by different organizations. Another important issue in terms of the system's reliability is that the information necessary for different non-biometric identification methods should be unique and preserved without duplication.

One more relevant aspect of the proposed Internet biometric system is that it works under any computer network environment, at any network point (terminal), and presents the same functionality, hiding as many operational details as possible that are not relevant to the users. Additionally, any reference information, either biometric or not, can be locally centralized or geographically distributed according to the convenience of applications.

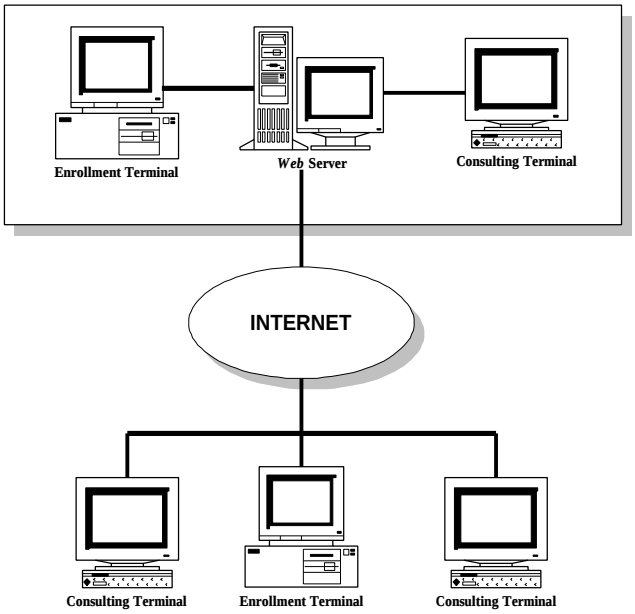


**Figure 1**. The automated Internet biometric system model for the enrollment, consultation and verification services.

The biometric identification, by its turn, in general involves with many different applications (security, immigration, access control, smart card, etc [4,5,6]). In the case of credit cards, for instance, a shop clerk can consult the desired information via the Internet to verify the authenticity of the signature provided by a client. For security application, any local police department is able to visualize in real time the desired biometric images of fingerprints and/or faces, and to access either fingerprint or face authentication service via the Internet, also in real time.

From a user's point of view, we expect that he/she is able to interact with the Internet biometric system by performing the following three operations through an Internet *Web* Page [9]: the enrollment, visualization (or consultation) and automatic verification. Within such an operational context, Figure 1 shows the proposed Internet biometric system model which consists of 3 network elements performing the three above mentioned tasks. In terms of network elements, these operations are carried out logically by three different functional network components below:

- ***Web* Server**: this network component is responsible for the management of network communication and the coordination of the exchange of information among related network terminals. In addition, *Web* Server also processes requests for accessing CGI programs (*enrollment*, *consulting* and *verification*).
- **Consulting Terminals**: through which the requests for consulting the database via *Web* Server are sent and *Web* server then grants the access to the database for the visualization or verification service.
- **Enrollment terminals**: which consists of special hardware and software capable of capturing biometric information.

## 3. THE SYSTEM IMPLEMENTATION

The prototype implementation was based on the system model described in Section 2. An essential component of this prototype is the Database Manager (DBM), responsible for maintaining the user's records and biometric data necessary for the implementation of different personal identification services. One of the interesting features of the implemented DBM is its capability of supporting both local and wide area network environments so that many users are able to access real time personal identification services simultaneously and remotely.

Another striking characteristic of the DBM is its flexibility in developing independent applications for each type of biometric features. Such an independent property allows the system to be used for a large variety of purposes at the same time. An example of this sort could be the situation where a local bank agency having an automated banking system available in a local area network and connected to a long distance network where the database containing the information about every bank client or clerk. From this local bank agency three banking services which involve different types of personal identification can be carried out at the same time: (1) a cashier via a signature verification module accesses the database and validates the signature on a bankcheck even the check was released by other agency; (2) The identification of a bank clerk can be done via a fingerprint module to authorize some important financial transactions and operations; (3) A client via a face verification module attached to an automated teller machine accesses a variety of banking services like cashing, money transfer, bill payment, etc. In this example, the advantage of maintaining a centralized database of every client and clerk that avoids a possible problem of violating database integrity becomes evident. Figure 2 illustrates the interaction between the DBM and different personal identification modules.

Each identification module consists of three sub-modules, named the enrollment sub-module, the visualization sub-module and the automatic verification sub-module. A request to the DBM for information by a biometric identification module is done via a SQL message. In this section we describe how these three sub-modules were implemented and show, as illustration, how a user accesses the biometric signature services**.** A detailed description of the implemented method for biometrics signature

information processing and feature extraction, as well as the implemented decision algorithm for automatic signature verification, can be found in a parallel submitted paper (Part II)

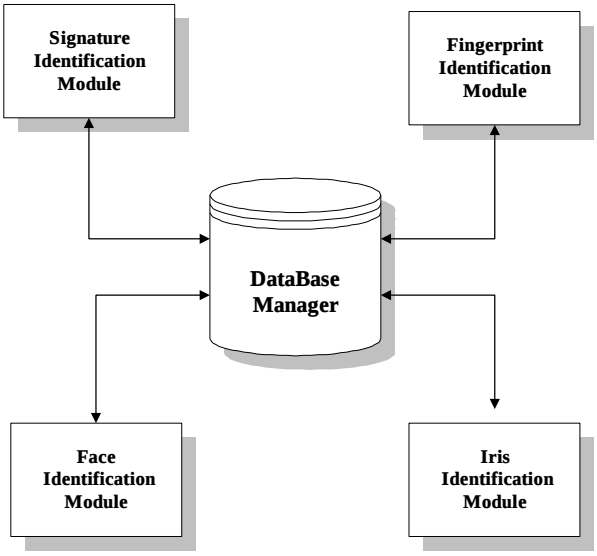


Figure 2. Interaction between the Database Manager and biometric modules

## 3.1 The Enrollment Sub-Module

This sub-module consists basically of 5 CGI programs, each one performing some specific function [14]. The messages sent by the Enrollment Sub-Module to the DBM are responsible for the creation of a profile for each new client during his enrollment (registration). If a client has not been enrolled before, a record of this client is generated. This is done by sending the following client's information: *client's name* (login), *client's identification number* (ID), three biometrics image sample files, the mean vector of the extracted biometrics characteristics obtained from these three samples images, and the desired decision threshold value. If, on the other hand, the DBM signals that the client has been registered previously, the user still has the chance to update this client's personal information on the database. Figure 3 shows the very first screen during an enrollment procedure where the user should provide client's name and ID number. Figure 4 shows a screen signaling the reception of the valid client information by *Web* Server and requesting that 3 reference biometrics sample images be submitted. The *browser* screen shown in Figure 5 guides the user through the submission of the first sample image. A similar *browser* screen illustrated in Figure 5 should appear still twice for the submission of 2 other biometric images. Notice that each *browser* screen like that in Figure 5 also has the goal of acknowledging the successful transfer of the previous sample image, and the screen as shown in Figure 6 declares the enrollment operation completed once the third biometric image was transferred with success.

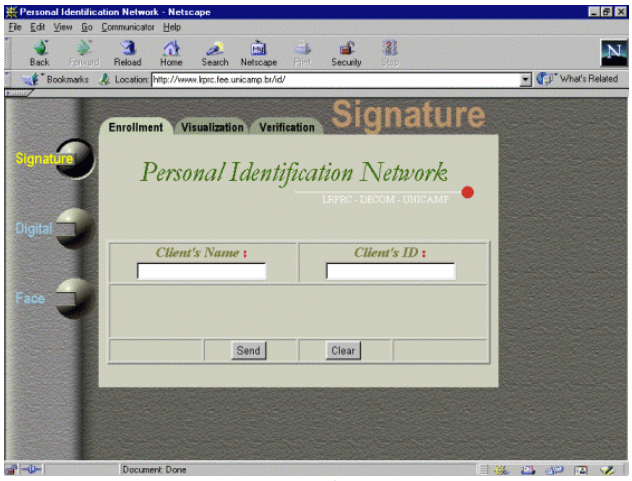


Figure 3: The initial screen of an enrollment procedure.

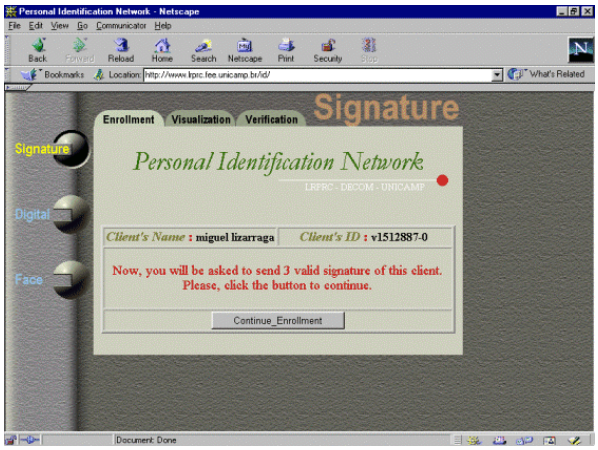


Figure 4: *Web* Server validating the received client's information and requesting the continuation of the ongoing enrollment process.

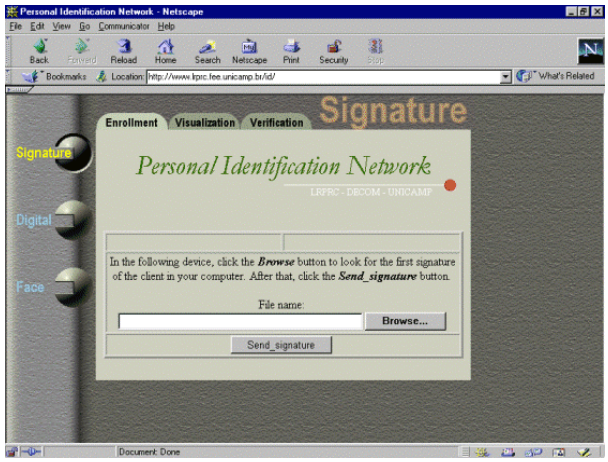


Figure 5: The *Browser* screen for the submission of the first biometric image.

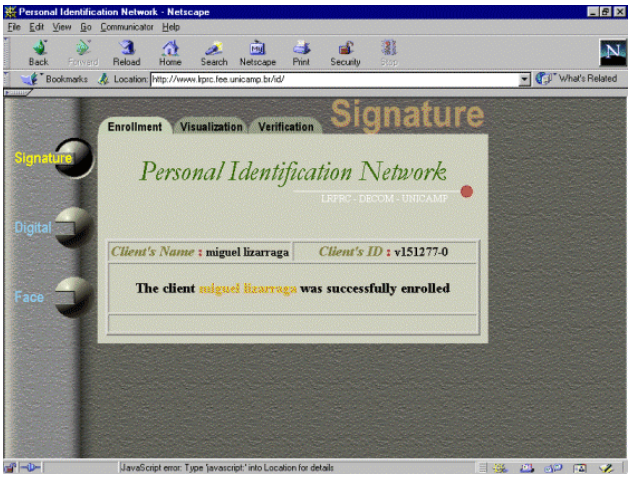


Figure 6: The new Client, *Miguel Lizarraga*, was successfully enrolled.

## 3.2 The Visualization Sub-Module

This sub-module is represented basically by a CGI program that allows a user to make a visual consultation of a reference biometrics image recorded previously during an enrollment procedure. For this end, the user activates Visualization *Tab* in the graphic interface, as shown in Fig. 7, and introducing then the client's name and ID number that are subsequently sent to the DBM by the visualization sub-module. In addition, the user also is able to specify the type of biometric image ("Signature", "Digital" or "Face") that he would like to see, and the DBM responds subsequently with an appropriate selected reference image according to the user's request. Figure 8 shows, as an example, how the biometric signature information returned by the DBM is displayed on a graphic interface screen.

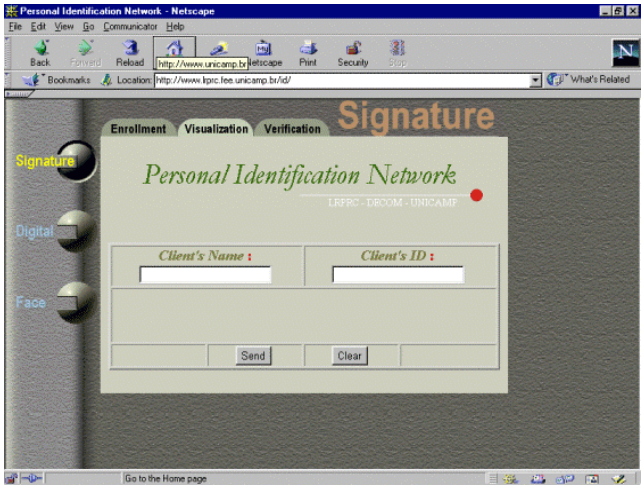


Figure 7: The consultation service is activated by pressing ***Visualization*** *tab*.

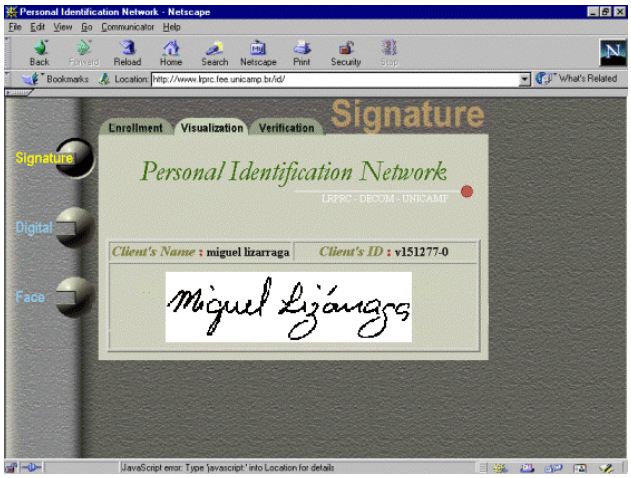


Figure 8: The graphic interface displaying a biometric signature image.

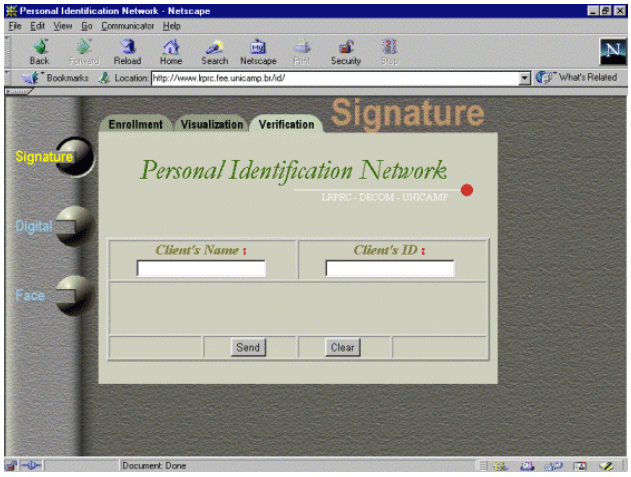


Figure 9: The verification service is activated by pressing ***Verification*** *tab*

## 3.3 The Automatic Verification Sub-Module

This sub-module consists basically of 3 CGI programs. The activation of ***verification*** *tab* sets the biometric system on the ***verification*** mode, as illustrate by the screen in Figure 9. To access the identity verification service, the user introduces both client's name and ID information. After successful validation of the provided client's name and ID number, a new screen instructing the user how to proceed the verification procedure is displayed. For our case of handwritten signatures, the screen of Figure 10 appears and the selection and the submission of a new signature image candidate proceed. Once *Web* Server has successfully received the submitted biometrics image, it starts immediately the verification work. Figure 11 shows an example of the submitted signature image being classified as a genuine one. This verification result is plausible only if the distance

measure between the reference biometrics sample and the submitted biometrics candidate is less than a pre-defined threshold value. Otherwise, the candidate signature is declared as a forgery.

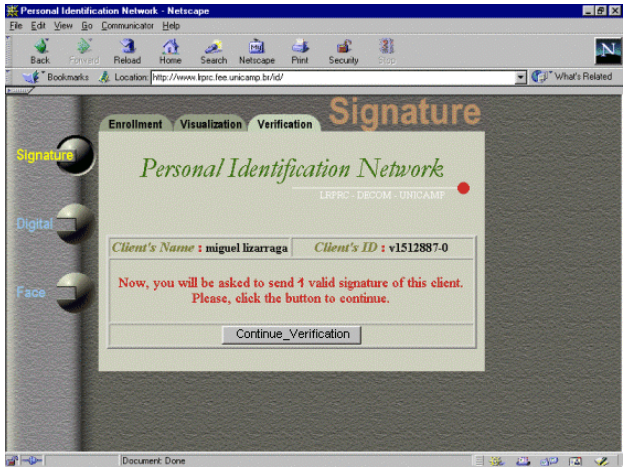


Figure 10: Client's information is validated and a candidate signature image is requested.

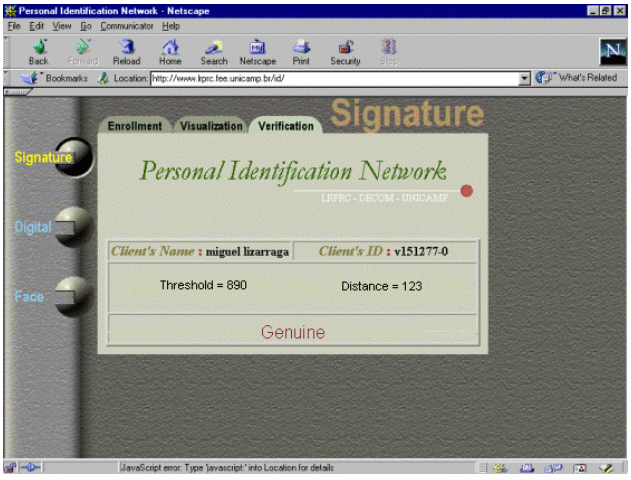


Figure 11: The candidate biometric signature image is classified as a genuine one.

## 4. CONCLUSIONS AND COMMENTS

We have found the increasing use of biometrics in conjunction with non-biometrics or sometime with some traditional personal identification methods. The choice of a specific biometric approach depends on the degree of security demanded by the applications. Biometric characteristics like fingerprints, faces and signatures can be easily and quick authenticated via the Internet. This is due to low cost and high efficiency of commercially available biometric sensors and the advance in biometric identification algorithms and electronics with the popularization of the Internet. In this paper we described the implementation of an Internet based personal identification system, named the Personal Identification Network, that offers two basic real time services via the Internet: visual consulting service and automatic personal verification service. The major goal of this work is to show the feasibility of providing real time biometric personal identification service via the Internet. In particular, a detailed description of the implementation of a real time automatic signature verification method based on a serial multi-expert and multi-resolution approach can be found in a parallel-submitted paper (PART II).

For future work, we intend to incorporate some already developed face and fingerprint verification algorithms into the Personal Identification Network [13,15]. Also we find interesting to incorporate on-line biometric image compression facilities for signatures and fingerprint into the Personal Identification Network. The fingerprint compression [15] and the handwritten signature compression [11] are based on Wavelet method and the runlength coding, achieving 20 to 1 and 95% losseless compression rates, respectively. Some benefits from using compression technique in our Internet based biometric system include: efficient use of storage devices, reduction of traffic load in the Internet.

## 5. REFERENCES


[1] O. Ureche, R. Plamondon. Document transport, transfer and exchange: security and commercial aspects, Proc. ICDAR 99, Bangalore, India, 1999, 585 – 588.

[2] J. Ashbourn, Biometrics – Advanced Identity Verification, Springer, 2000.

[3] D. Zhang, 2000, Automated Biometrics: Technologies & Systems, Kluwer Academic Publishers, USA.

[4] T. Pegoraro, Tarciano, Robust voice recognition algorithms applied to speaker verification, MS Thesis, FEEC-Unicamp, April 2000.

[5] M. C. Fairhurst, Signature verification revisited: promoting practical exploitation of biometric technology, Electronics and Communication Engineering Journal, December (1997) 273 – 280.

[6] A. Jain, A., L. Hong L, S. Pankanti, Biometrics: promising frontiers for emerging identification market, Communication of ACM, February (2000) 91 – 98.

[7] A. Jain, A, S. Prabhakar, A. Ross, Biometrics-based web access, Technical Report: MSU-CPS-98-33, Michigan State University, 1998.

[8] D. Maio, D. Maltoni, A secure protocol for electronic commerce based on fingerprints and encryption, Proc. ISAS'99, 4 (1999) 519-525.

[9] I. Ricarte, An introduction to Web processing mechanism, URL: http://ww.dca.fee.unicamp.br/~ricarte. (In Portuguese)

[10] M. G. Lizárraga, An automatic system for static signature consultation and verification, MS. Thesis, State University of Campinas –UNICAMP, 1996. (In Portuguese)

[11] K. Leong, T. Srikanthan, G. Hura, An Internet application for on-line banking", Computer Communication, 20 (1998) 1534 – 1540.
[12] E. L. Andrade Neto, L. L. Lee, A face recognition system based on principal component analysis, Brazilian Telecommunications Magazine, 13 (1), (1998) 56-63. (In Portuguese)
[13] L. H. Leskow, Automatic fingerprint image compression, Technical Report, DECOM-FEEC-UNICAMP, 1997. (In Portuguese)
[14] M. G. Lizárraga, Biometric personal identification via the Internet with emphasis on static signatures, Ph.D. Thesis, State University of Campinas –UNICAMP, August 2000. (In Portuguese)
[15] L. H. Leskow, Automatic fingerprint image compression and verification, Ph.D. These, DECOM-FEEC-UNICAMP, to be completed by August 2001. (In Portuguese)