Retinal Based Authentication via Distributed Web Application

C. Mariño, M.G. Penedo, and M. Penas

Grupo de Visión, Artificial y Reconocimiento de Patrones, (VARPA),
Universidade de A Coruña, Campus de Elviña s/n
castormp@fi.udc.es, {cipenedo, infmpc00}@dc.fi.udc.es

Abstract. Traditional authentication systems, employed to gain access to a private area in a building or to data stored in a computer, are based on something the user *has* (an authentication card, a magnetic key) or something the user *knows* (a password, an identification code). But emerging technologies allow for more reliable and comfortable for the user, authentication methods, most of them based on biometric parameters. Much work could be found in literature about biometric based authentication, using parameters like iris, voice, fingerprints, face characteristics, and others. We have developed a new methodology for personal authentication, where the biometric parameter employed for the authentication is the retinal vessel tree, acquired through a retinal angiography. It has already been asserted by expert clinicians that the configuration of the retinal vessels is unique for each individual and that it does not vary in his life, so it is a very well suited identification characteristic. In this work we will present the design and implementation stages of an application which allows for a reliable personal authentication in high security environments based on the retinal authentication method.

1 Introduction

Reliable authentication of people has long been an interesting goal, becoming more important as the need of security grows, so that access to a reliable personal identification infrastructure is an essential tool in many situations (airport security controls, all kinds of password-based access controls, ...). Conventional methods of identification based on possession of ID cards or exclusive knowledge are not altogether reliable. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised. A solution to that problems has been found in the biometric based authentication technologies. A biometric system is a pattern recognition system that establishes the authenticity of a user's specific physiological or behavioral characteristic. Identification can be in the form of verification, authenticating a claimed identity, or recognition, determining the identity of a person from a database of known persons (determining who a person is without knowledge of his/her name).

Many authentication technologies can be found in the literature, with some of them already implemented in commercial authentication packages [1,2,3]. But today most of the efforts in authentication systems tend to develop more secure environments, where it is harder, or ideally, impossible, to create a copy of the properties used by the system to discriminate between authorized individuals and unauthorized ones, so that an impostor

R. Moreno Díaz et al. (Eds.): EUROCAST 2005, LNCS 3643, pp. 386–391, 2005.

could be accepted by the biometric system as a true sample. In that sense, the method employed by our system [4] uses as the authentication biometric parameter the blood vessel pattern in the retina of the eye.

In this paper, a distributed client-server framework which allows for personal authentication is outlined. From the design stage, where design patterns are the fundamental tool, to the implementation (server, communication channels and clients) are described. The main goal of this work is to build a robust system which allow for the automatic personal authentication, which would allow or deny the access to critical resources of the system.

2 Authentication Methodology

In many cases it is almost impossible to acquire the biometric parameter in the same conditions than the stored template used for the authentication, so that a first step of normalization of both parameters (the acquired and the reference one) is needed in order to make the system reliable enough, avoiding the rejection of legitimate users by changes due to illumination, translations or rotations in the image. The main drawback of retinal angiographies is the different position of the vessels used in the authentication, because it is very difficult that the user places the eye in the same position in different acquisitions, so that an alignment is necessary prior to the authentication. To perform that alignment, an image registration algorithm is employed [5].

Here a feature-based authentication method is employed, as commented in [4], where features are extracted from the angiographies using a differential geometry operator (Figure 1), the MLSEC-ST [6, 7], and then a multi-resolution alignment algorithm is performed until both images (the reference image, stored in the database and the acquired image) are registered. Finally, similarity between the aligned images is measured by means of the Normalized Cross-Correlation Coefficient [8] γ, and if the value γ is higher than the acceptance threshold the individual is accepted, or rejected otherwise.

The whole authentication process is depicted in Figure 2. Firstly, in the *enrollment* stage, authorized individuals are entered in the database. After that, each time the user requests for a resource or for accessing to a protected area, the authentication process is performed (second stage).

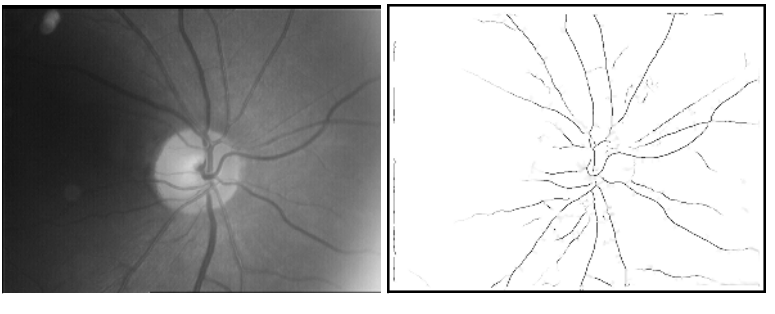

Fig. 1. Features extracted from angiographies are employed as the reference points in the registration process. (a) Original angiography. (b) Creases extracted from (a).

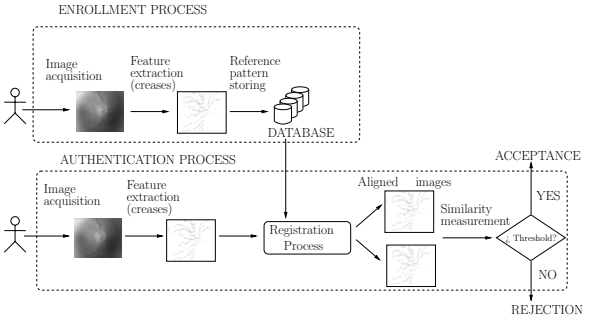

Fig. 2. Representation of the authentication process, composed by two stages: an initial enrollment stage, where the reference pattern is stored in the database of authorized users, and an authentication step, which is performed each time the individual requests for a protected resource

3 Description of the Distributed System

Our system employs a conventional client-server architecture [9]. Once the retinal pattern of the authorized person is stored in the database, the system performs an authentication procedure each time the individual tries to access to the protected resources of the system.

To fulfill the main requirements of the system, a framework which allows the communication between the server authentication system and the acquisition device located at the access points must be designed. That communication must be above all reliable and secure. That two requirements could be solved by means of a secure communication protocol, such as Secure Socket Layer (SSL) communications (Figure 3).

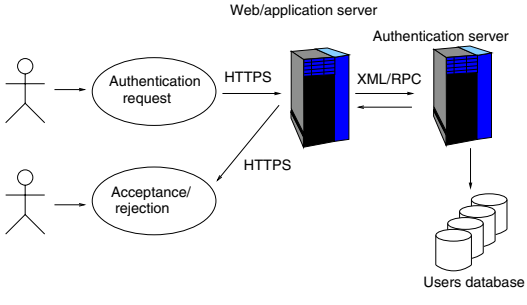

Fig. 3. The distributed authentication system

The most important tools employed for designing the system were the design patterns [10] and the UML [11, 12], which allow for a more robust and reliable software applications. For example, the strategy pattern encapsulates several methods employed to authenticate the individuals (although, by the moment, only the one described here has been reliably tested). But also distributed patterns appeared in the design: single

threaded execution pattern is needed to allow only a client updates the data in the authorized people database at a time or the read-write lock pattern, which avoids unnecessary waiting to read data from the database by allowing concurrent reads when data are being updated.

A client application initiates a connection to authenticate an individual, and if authentication is successful, resources can be accessed. The graphical user interface for the interaction with data (like the depicted in Figure 4) is obtained through the web application.

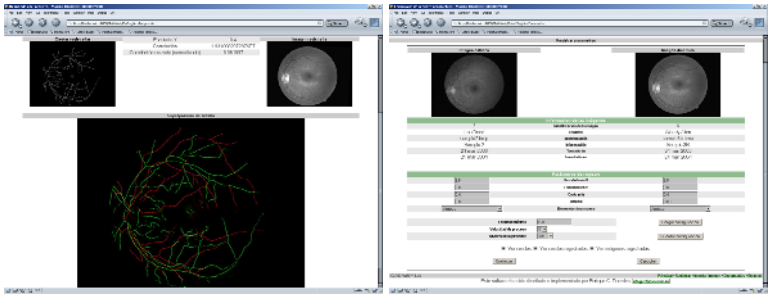

Fig. 4. Screenshots from the client program-application with retinographies, which are the biometric authentication parameter employed by the system. (a) Extracted features employed by the system. (b) Authentication parameters obtained in a typical access situation.

The overall operation flow at the client-side can be described as follow (see also Figure 3):

- An individual makes HTTP request to web server first. The web server will handle the request and will communicate with the authentication server to perform the authentication process.
- The authentication server will access the database and will allow or deny the access to the requested resource. Upon request, procedure execution will be invoked (using XML-RPC) based on the data sent by the client.
- Once the procedure ends, the related information is sent to the client and displayed in the browser window, allowing or denying access depending on the result of the authentication process.

4 Communication Technology

To assure confidentially and reliability in the communications, the most widely used secure Web encryption has been employed: the Secure Hypertext Transport Protocol (HTTPS) on the Secure Socket Layer (SSL) version 3.0 with 40 and 128 bit RC4 encryption. The SSL [13] protocol has become most widely used method for encrypting and authenticating Web communications.

Our approach to deal with the heterogeneity of the clients focuses on documents or data and transformations that visualize the data to fit the computing capabilities

of different users, while preserving semantics of data. This division of the underlying data and the way it gets displayed mimics the Model-View-Controler (MVC), a well known and frequently used design pattern to develop interactive applications with flexible human-computer interfaces. This would allow for a future implementation of mobile authentication clients, for example.

XML has been chosen as the medium to represent the data sent to the server for the authentication. XML is a markup language for documents containing structured information. Once the data is written in XML, an associated XSL document can be written to define the way it gets displayed. The XML document is platform-independent and thus corresponds to the *model*, whereas the style sheet depends on the displaying device, and corresponds to the view.

MVC separation of view and model offers the following advantages over conventional application-centric environments:

- Model-view separation at the document level via XML/XSL documents.
- Simple communication protocol with a standard message format based on (encrypted) ASCII XML messages.

Finally, using XML-RPC [14], procedure calls are wrapped in XML establishing that way a simple pathway for calling authentication functions. XML-RPC is a quick-and-easy way to make procedure calls over the Internet. It converts the procedure call into XML document, sends it to a remote server using HTTP, and gets back the response as XML. Other considered (although finally discarded) protocols where SOAP and CORBA, both of them popular protocols for writing distributed, object-oriented applications, well-supported by many vendors, although they are much more complex than XML-RPC, and require fairly sophisticated clients. In addition, XML-RPC has fewer interoperability problems than them.

5 Conclusions and Future Work

In this paper an authentication web application has been presented. Using that program restricted access to system resources (buildings, data, etc.) can be granted only to authorized individuals, rejecting those requests from unauthorized persons. XML, which serves as the communications medium, is a standard that has already gained wide acceptance and provides a powerful medium for data exchange, visualization specifications and procedure execution by means of the XML-RPC method invocation procedure. Moreover all the communications take place over secure channels, through to the employment of encryption with HTTPS on the SSL version 3.0. Currently, system is under evaluation and many tasks as robustness assessment, performance verification, formal verification of whole the server-procedures, so as testing in a real environment must be performed.

Acknowledgments

This paper has been partly funded by the Xunta de Galicia through the grant contract PGIDIT03TIC10503PR

References

1. J.G. Daugman. Biometric personal identification system based on iris analysis. United States Patent No.5,291.560, 1994.
2. J.Bigüin, C.Chollet, and G.Borgefors, editors. *Proceedings of the 1st.International Conference on Audio- and Video-Based Biometric Person Authentication*, Crans-Montana,Switzerland, March 1997.
3. R. Zunkel. Hand geometry based verification. In *BIOMETRICS:Personal Identification in Networked Society*. Kluwert Academic Publishers, 1999.
4. C. Mariño, M.G. Penedo, and F. González. Retinal angiographies based authentication. *Lecture Notes in Computer Science*, 2905:306–313, 2003.
5. L.G. Brown. A survey of image registration techniques. *ACM Computer Surveys*, 24(4):325–376, 1992.
6. A. López, D. Lloret, J. Serrat, and J.J. Villanueva. Multilocal creasness based on the level set extrinsic curvature. *Computer Vision and Image Understanding*, 77:111–144, 2000.
7. C. Mariño, M. Penas, M.G. Penedo, D. Lloret, and M.J Carreira. Integration of mutual information and creaseness based methods for the automatic registration of slo sequences. In *Proceedings of the SIARP'2001, VI Simpósio Ibero-Americano de Reconhecimento de Padrões*, volume I, 2001.
8. J.P.Lewis. Fast template matching. *Vision Interface*, pages 120–123, 1995.
9. Robert Orfali, Dan Harkey, and Jeri Edwards. *Client/Server Survival Guide.* John Wiley & sons, 3rd edition, 1999.
10. E. Gamma, R. Helm, R. Johnson, and Vlissides J. *Design Patterns, Elements of Reusable Object-Oriented Software*. Professional Computing Series. Addison-Wesley, 1995.
11. Mark Grand. *Patterns in Java: a catalog of reusable design patterns illustrated with UML*, volume 1. New York,John Wiley & sons, 1998-1999.
12. Mark Grand. *Patterns in Java: a catalog of reusable design patterns illustrated with UML*, volume 1. New York,John Wiley & sons, 1998-1999.
13. K.E.B. Hickman. The SSL protocol. http://www.netscape.com/newsref/ssl.html, December 1995.
14. Simon St.Laurent, Joe Johnston, and Edd Dumbill. *Programming Web Services with XML-RPC*. O'Reilly, 2001.