Biometrics-Based Web Access*

A. K. Jain, S. Prabhakar, and A. Ross
Department of Computer Science and Engineering
Michigan State University, East Lansing, MI 48824
{jain,prabhaka,rossarun}@cse.msu.edu

Abstract

Authentication and encryption are crucial to network security. Public key cryptography provides a secure way to exchange information but designing a high security authentication system still remains an open problem. Complex passwords are easy to forget while simple passwords are easily guessed by unauthorized persons. Several of the biometric characteristics of an individual are unique and do not change over time. These properties make biometrics well suited for authentication. Authentication systems based on fingerprints, voice, iris, and hand geometry exist for applications such as passport control, forensics, automatic teller machines, driver license, and border control. With the increasing growth of the Internet, there is a need to restrict access to sensitive data on the Web to authorized users. We have developed a prototype system which uses hand geometry to authenticate users to restrict access to web pages. Initial evaluation of the prototype system is encouraging. Similar techniques can be used to authenticate people for e-commerce applications.

Keywords: Biometrics, Internet applications, network security, authentication, encryption, hand geometry, Web pages

1 Introduction

It was not long ago that system security issues took a back seat to system performance. Today, there is an increased need for network security as our society is becoming more tightly interconnected. With a massive surge of interest in the Internet and the availability of low-cost residential broadband networking for homes and small enterprises, more and more people have access to the Internet. There is a huge amount of sensitive commercial, personal, military and governmental information on the Internet that needs to be secured so that only authorized people can gain access. Web services depend on Internet Protocol (IP) name service. If an imposter gains access to the name service, the security based on correlating names and network addresses will fail. The

*This work is partially supported by IBM contract No. 44400469.

traditional method of authentication requires a username and password which is transmitted openly across a network. The risk of password eavesdropping can be reduced by the use of encryption technologies.

Biometrics [1] is an emerging technology which authenticates users by their physical and behavioral characteristics and obviates the need to remember a password. It also requires the person to be authenticated to be physically present at the point of authentication. Biometrics, together with encryption is capable of providing foolproof security for Web access and e-commerce. There is an increasing trend to use biometrics in conjunction with other technologies for security. The additional cost of biometric sensors needs to be reduced and consistency and reliability of feature extraction and matching algorithms improved for this to be feasible. Some of the biometric sensors, e.g., a camera and a microphone are becoming low-price standard options on PCs. Stamp-size solid state fingerprint capture devices are expected to become very cheap ($\sim$ \$10) and may soon be available on laptops [2]. With an expected drop in the price of biometric readers and an emerging need for security, biometric authentication will become very popular in the near future.

In this paper we address the issue of biometric-based access to the Web. The feasibility of such a system is demonstrated by designing a prototype system which uses hand geometry [3, 4] to verify a user and give him access to particular files on the Web. Any other biometric [5] (e.g., fingerprint and speech) may be used in a similar way. Similar systems based on fingerprint [6] and face [7] may soon be available commercially. Another system based on speaker verification [8] can be modified and used to restrict access to the Web.

2 Motivation and Assumptions

Basic Authentication [9] is a NCSA (National Center for Supercomputing Applications) method of authentication which restricts access to HTML documents and server directories to those visitors who give a valid username and password. This feature allows webmasters to restrict access to certain directories. The usernames and encrypted passwords are kept in a webmaster-maintained file. Authentication based on passwords is susceptible to compromise by an imposter, particularly since the user need not be present at the point of authentication. Passwords can also be forgotten. Biometrics, which refers to authentication of people based on their physiological or behavioral characteristics is inherently more reliable and has a higher discrimination capability than the knowledge-based approaches (i.e., knowing the passwords), because the biometric characteristics are unique to each person. We will demonstrate that it is feasible to design a biometric-based access mechanism for the Web.

In Basic Authentication [9], the password is transmitted over the network as a "uuencoded" string rather than encrypted. So, the password can be easily decoded by someone who is able to capture the right packet. There are utilities available which can easily find such packets. More secure authentication can be provided by sending the password encrypted. A system based on biometrics must also transmit data back to the server which can be done using encryption. An even more secure method is

to use a dual-key encryption system where one of the keys is derived from the sensed biometric itself. In this paper, however, we will not concern ourselves with this issue. For simplicity, let us assume that the information is transmitted over the network in a secure way. The issue is to provide a more secure *authentication*. Our system still uses Basic Authentication [9] as provided by NCSA to restrict access to the web server directories, but uses biometrics instead of passwords for authentication. With the increasing acceptability of biometrics, we anticipate that such a facility will be integrated in the NCSA HTTPD (Hyper Text Transfer Protocol Daemon) and will become a standard.

Choosing a specific biometric is a major design issue. Each biometric has its own strengths and limitations, and accordingly each biometric is suitable for a particular authentication application. The fingerprint-based authentication systems are very popular in high security applications. There are, however, number of privacy issues associated with transferring fingerprints over the network. Fingerprints reveal far too much information about a person's identity. We have chosen to use hand geometry for the task of verification because hand geometry is distinctive enough for verification but not very accurate for identification. Further, people appear to be more comfortable in giving their hand geometry measurements rather than their fingerprints. Our system only verifies whether the user is indeed who he claims to be.

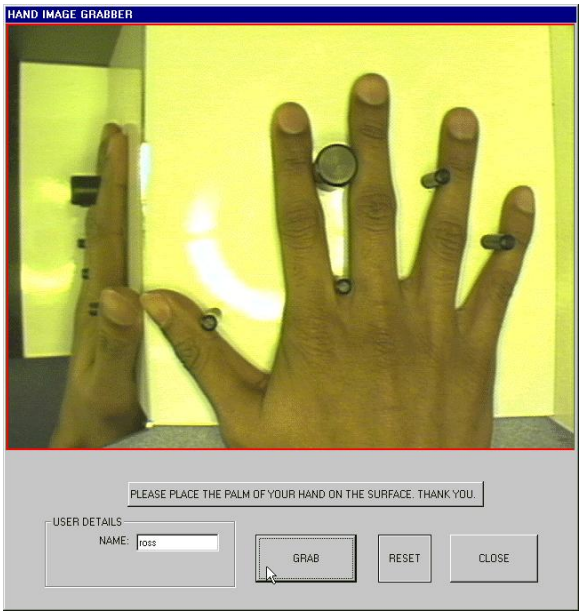

Figure 1: The GUI to capture hand geometry.

3 System Design

Our system can be logically divided into two independent modules. The first module is the hand geometry-based authentication system, and the second module deals with the client-server interaction to restrict/grant access to the web. We first describe the hand-geometry based authentication system which is essentially a pattern recognition system. We have developed a prototype system and have tested it on a database acquired in a laboratory environment. Currently, we are working on algorithms to improve the system performance and verification speed of our system. The second module is the client-server interaction that exchanges hand geometry data and restricts access to certain HTML documents.

3.1 Hand geometry-based verification system

We first briefly outline our user authentication system which is based on a set of hand geometry features. The acquisition system comprises of a light source, a camera, a single mirror and a flat surface (with five pegs on it). The user places his right hand on the surface - palm facing down (people with a disability in right hand can place their left hand on the surface - palm facing up). The five pegs serve as control points for appropriate placement of the user's hand. The mirror provides a side view of the hand. A GUI is developed to provide live visual feedback of the top and side views of the hand. In the current prototype implementation, a 640×480 8-bit grayscale image of the hand is acquired (Figure 1). The two main modules in a hand geometry based verification system are: (a) the enrollment module and (b) the verification module. These two modules are described below.

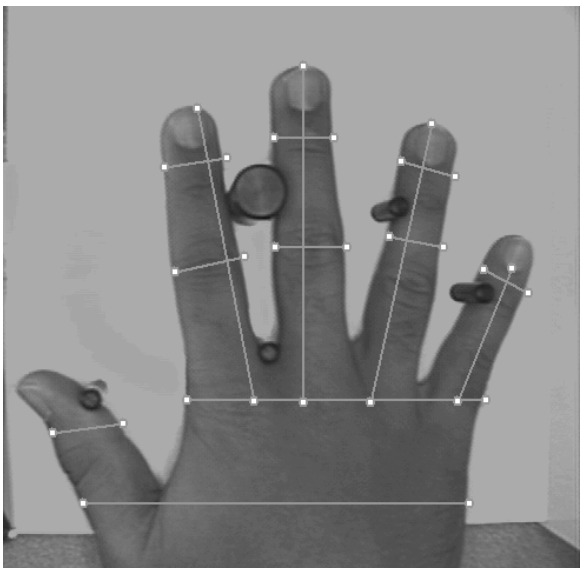

Figure 2: Features extracted from the image of a hand.

3.1.1 Enrollment

Every user who wishes to access a web page must first enroll himself. The enrollment module is used to add a new user to the database or update a current user's profile or feature vector. During enrollment, five images of the same hand are captured. A feature vector is extracted for each hand image. The five feature vectors are stored as templates in the database for each user. The sixteen geometric features extracted from each image are typically the lengths and widths of the fingers, aspect ratio of the palm or fingers, thickness of the hand, etc. Figure 2 illustrates the sixteen geometric features extracted from a hand.

3.1.2 Verification

Verification involves matching the features extracted from the given hand to template of the same person previously enrolled in the system. In our system, a snapshot of the hand is taken, geometric features are calculated using the same algorithm as in the enrollment module and the resulting feature vector is compared with those stored in the database for the person to be verified.

3.2 Restricting Access on Web

Our access mechanism uses the NSCA's standard Basic Authentication [9] to restrict access to a web directory. Figure 3 shows the client/server interaction for the enrollment and access of secure pages. Only one file (e.g., index.html) is allowed access in the directory. This file, when downloaded to the client side, prompts the user to provide his hand geometry for authentication. The dialog box which provides live feedback of the hand geometry is an ActiveX control which can access system resources. This control captures the hand geometry image, calculates the feature vector and sends it to the server along with other information about the user without storing it on the client's disk. This way, transmission of the feature vector is transparent to the user and the user has to be present at the point of authentication. This information is sent to the server as a digitally signed form. Currently, a Java applet cannot access system resources, therefore, we have made use of an ActiveX control to capture the hand geometry image. Since the feature vector is sent across the network, an imposter could listen to the channel and capture the feature vector. To avoid this, public key encryption methods should be used.

Once the server has the hand geometry information about a user along with the user name, the server invokes the hand geometry authentication module to verify the user. If the authentication fails, the client is denied access to the files and this information is conveyed to the client (Figure 4 (b)). If the access is allowed (Figure 4 (a)), then the server retrieves all the filenames accessible to this user and displays them as a list. The client can then access these files by clicking on their names in the browser. The secure files do not reside in a world readable directory and hence cannot be accessed through a URL. The server reads the file the user has requested (by clicking on one of the filenames) and dynamically generates an HTML file containing the contents.

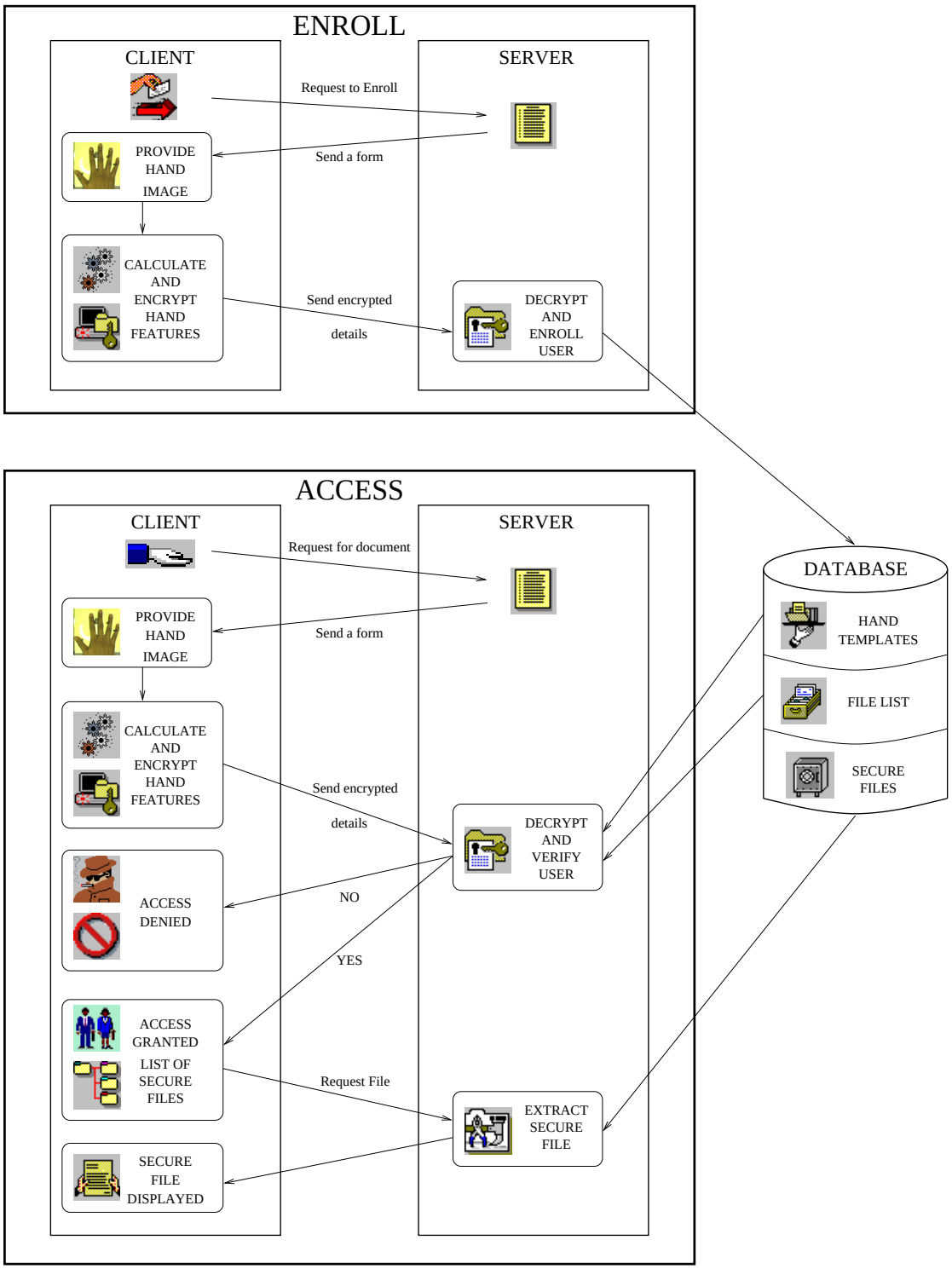

Figure 3: Flow diagram of client-server interaction.

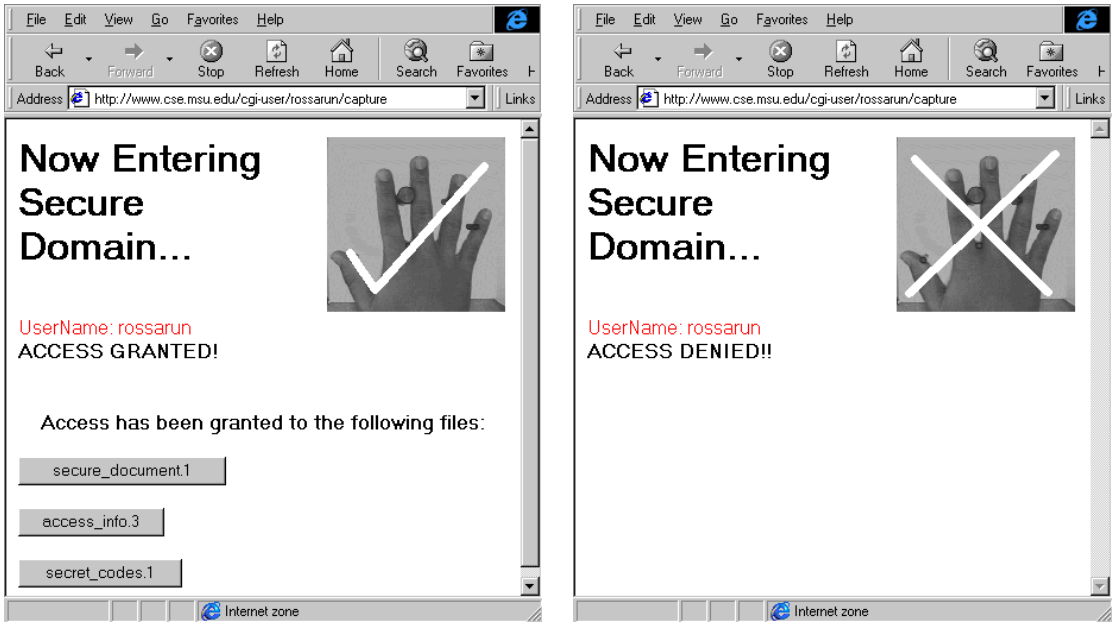

Figure 4: Authentication GUI. (a) When access is granted, a list of accessible files is presented to the user. (b) When access is denied, user can not access any file.

4 Experimental Results

We have designed two experiments to evaluate our system. The first experiment tested our prototype hand geometry-based authentication system using a database of hand geometry images of 50 users acquired in our laboratory. A total of 10 images of the right hand of each user were captured in two different sessions. Our current acquisition system does not provide any user training for a proper placement of the hand. No instructions were given to the users about the proper placement of their hands. Out of a total of 500 images, 140 images were discarded because of incorrect placement of the hand. The remaining 360 images were used in our experiments. A genuine matching score is obtained by comparing the feature vectors from the same hand while an imposter matching score is obtained by comparing the feature vectors from two different hands. In order to study the performance of the system the Receiver Operating Curve (ROC), which plots the authentic acceptance rate (1-FRR) versus the false accept rate (FAR) was plotted. The ROC for our experiments is shown in Figure 5.

The second experiment was designed to test the performance of the overall web access system. Ten files were created in a web directory and *Basic Authentication* [9] was used to restrict access to this directory. Ten users were asked to evaluate the system. Seven out of the ten users were enrolled into the system. Each of the seven enrolled users was allowed to access a subset of the ten files. Over a period of three weeks, enrolled users accessed their files by providing their hand image each time. A

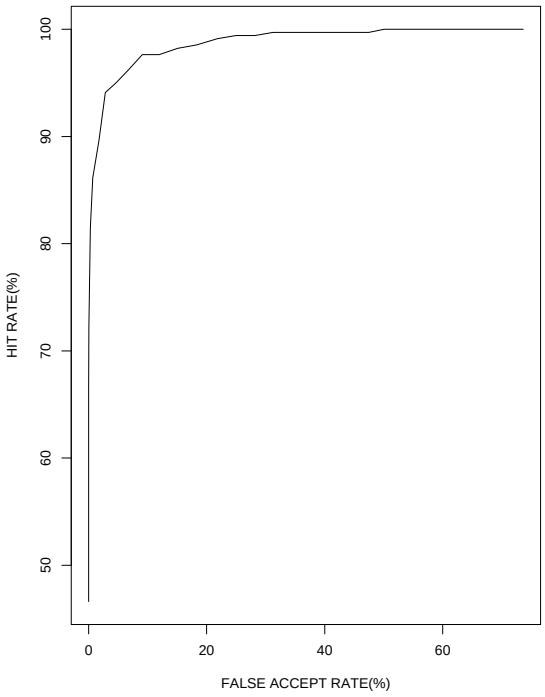

Figure 5: Receiver Operating Curve.

user accessing a set of files was not aware of the existence of the other files. The users were challenged to access other files or access the files without providing their hand geometry but none of these attempts were successful. Access to the files could not be gained in any way other than providing genuine hand geometry images. Each of the enrolled user also tried to enter the system by impersonating the other six users, while the three users who were not enrolled tried to enter the system as one of the seven enrolled users. In this experiment, we operated our hand geometry system at a threshold near the at the knee in the curve shown in Figure 5; this threshold gives an FRR of about 15% and an FAR of about 2% on the database used in the first experiment. For the ten users in the second experiment (200 authentic trials and 200 imposter trials), a FAR of 0% and FRR of 5% were obtained.

On a relatively small database of 50 people, the system performance is reasonable. The system should be extensively field tested on a large database before making any strong claims. The system performance is known to degrade with extended use of the system in the field because of accumulation of dust around the pegs. We are still investigating these aspects as well as our feature extraction and matching algorithms to improve the system performance.

5 Conclusions

Biometrics is expected to be increasingly used in conjunction with other technologies like the knowledge-based authentication (e.g., passwords and PIN) on the Internet. We have demonstrated that hand geometry-based authentication can be used to restrict access to web pages. The prototype system with seven registered users shows promising results. Our tests, conducted on a small database, support our claim that our system is secure. The choice of biometric depends on the security demand of the application and user acceptance. Fingerprint, voice, and face are the most suitable biometrics for restricting access to web pages as the sensors for these biometrics are small, cheap, and available as standard options on PCs from many computer vendors. Before a system is installed for commercial use, tests should be performed on a database involving a large number of users over a period of time. We are also working on developing authentication systems using other biometrics like fingerprints, voice, and face and integrating multiple biometrics for better performance.

Acknowledgments

Discussions with Scott Connell of the PRIP lab., Michigan State University and Yatin Kulkarni of Veritel Corporation are gratefully acknowledged. Dr. Sharath Pankanti of IBM T.J. Watson Research Lab. helped us in the design of the hand geometry-based verification system.

References

[1] E. Newham, *The Biometric Report*. New York: SBJ Services, 1995. http://www.sjb.co.uk/.

[2] Solid-state fingerprint capture devices from Veridicom. http://www.veridicom.com/.

[3] Anil K. Jain, A. Ross, and S. Pankanti, "A Prototype Hand Geometry-Based Verification System", to appear in the *2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication*, Washington D.C., March 22-24, 1999.

[4] R. Zunkel, "Hand geometry based verification", Biometrics: Personal Identification in Networked Society, Anil K. Jain, R. Bolle, and S. Pankanti, editors, Kluwer Academic Publishers, 1998.

[5] Anil K. Jain, R. Bolle, and S. Pankanti (eds), Biometrics: Personal Identification in Networked society, Kluwer Academic Publishers, 1998.

[6] Secure Web access control : MistyGuard (TRUSTWEB). http://www.mitsubishi.com/ghp_japan/misty/trustweb_e.htm.

[7] Access the Web with your face. http://www.miros.com/web_access_demo_page.htm.

[8] Online VoiceGuardian. http://www.keyware.com/Demos/index.html.

[9] NCSA HTTPD Mosaic User Authentication Tutorial. http://hoohoo.ncsa.uiuc.edu/docs/tutorials/user.html

[10] Ed Tittel, M. Gaither, S. Hassinger and M. Erwin. Web Programming Secrets with HTML, CGI, and Perl, IDG Books Worldwide, 1996.