Biometrics and Vein Map Authentication

Felix Fuentes, Dulal Kar, and Mario A. Garcia
Texas A&M University-Corpus Christi
mario.garcia@tamucc.edu

Abstract

There is increasing demand world-wide, from government agencies and the private sector for cutting-edge biometric security technology that is difficult to breach. Some older tools, such as fingerprint, retina and iris scanning and facial recognition software have all been found to have flaws. However, reproducing a three-dimensional model of a human vein system is impossible to replicate. Mapping veins as a human barcode is the newest technology to hit the security world which has key benefits over older technologies. Vein map technology is distinctive because of its state-of-the-art sensors are only able to recognize vein patterns if hemoglobin is actively flowing through the person's veins. Additionally, each individual's vein map is unique, even in the case of identical twins. The combinations of these factors could give vein map authentication an edge over existing biometric identification products.

1. Introduction

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are the: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice [8]. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. The term “biometrics” is derived from the words “bio” (life) and “metrics” (to measure). Automated biometric systems have only become available over the last few decades, due to significant advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds of years ago [20] .

Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. [5] Possibly the first known example of biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer Joao de Barros. He wrote that the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another. This is one of the earliest known cases of biometrics in use and is still being used today [2].

Elsewhere in the world up until the late 1800s, identification largely relied upon "photographic memory." In the 1890s, an anthropologist and police desk clerk in Paris named Alphonse Bertillon sought to fix the problem of identifying convicted criminals and turned biometrics into a distinct field of study. He developed a method of multiple body measurements which got named after him (Bertillonage) [2]. His system was used by police authorities throughout the world, until it quickly faded when it was discovered that some people shared the same measurements and based on the measurements alone, two people could get treated as one. After the failure of Bertillonage, the police started using finger printing, which was developed by Richard Edward Henry of Scotland Yard [17], essentially reverting to the same methods used by the Chinese for years.

To date, popular biometric authentication systems include, fingerprint identification, retina and iris scan, face recognition, and voice analysis. The problem with each system is that most can be breached easily or intrude upon the rights of individuals or both. Fingerprint identification is one of the most well-

known and publicized biometrics. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming automated due to advancements in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers), available for collection, and their established use and collections by law enforcement and immigration. A fingerprint appears as a series of dark lines that represent the high, peaking portion of the friction ridge skin, while the valleys between these ridges appears as white space and are the low, shallow portions of the friction ridge skin. Fingerprint identification is based primarily on the minutiae, or the location and direction of the ridge endings and splits along a ridge path. In over one hundred forty years of comparison worldwide, no two fingerprints have ever been found to be alike, not even in those of identical twins [15]. However, experiments performed over time have revealed that fingerprint scanning could be easily tricked. One such method revealed that by simply breathing upon traces of fat left by fingerprints on the scanner's surface revealed contours of the old fingerprint on the protected PC and granted access [12]. Also, the gathering of fingerprints is associated with criminal behavior in the minds people and is rejected by many.

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The automated method of iris recognition is relatively young, existing in patent only since 1994. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle. Although the coloration and structure of the iris is genetically linked, the details of the patterns are not. The iris develops during prenatal growth through a process of tight forming and folding of the tissue membrane [7]. Prior to birth, degeneration occurs, resulting in the pupil opening and the random, unique patterns of the iris [16,18]. Although genetically identical, an individual's iris are unique and structurally distinct, which allows for it to be used for recognition purposes. Such a complex system as the iris has also been proven to fail under experimentation. One such experiment authenticated an unauthorized person into the system by simply holding an ink-jet print-out over their eye [1,3,4]. The page was a printout of an authentic iris with a small hole cut into the page through which the pupil of the imposter was visible to the camera [12]. People often use faces to recognize individuals and advancements in computing capability over the past few decades now enable similar recognitions automatically [19]. Early face recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes [9,10,14]. Major advancements and initiatives have propelled face recognition technology into the spotlight. Face recognition can be used for both verification and identification. There are two predominant approaches to the face recognition problem: geometric (feature based) and photometric (view based). As researcher interest in face recognition continued, many different algorithms were developed, three of which have been well studied in face recognition research: Principal Components Analysis (PCA), Linear Discriminant Analysis (LDA), and Elastic Bunch Graph Matching (EBGM)

The goal of any access control system is to authenticate authorized people, not just their credentials, into specific places or allow then to perform specific tasks. Only with the use of a biometric device can this goal be achieved. A card-based access system will control the access of authorized pieces of plastic, but not who is in possession of the card. Systems using PINs require an individual only know a specific number to gain entry; but who actually entered the code cannot be determined. As opposed to using badges, sign-ins or other ways of tracking employees, a biometric time clock assures that no employee can punch in for another, eliminating time fraud and reducing payroll costs. Because every person's biometric characteristic is unique, a biometric time clock provides a quick, accurate, and reliable way to record in- and out-punches for each employee. That's why so many companies now employ biometrics. Issues in biometrics range from cultural, social, and religious issues depending on where the biometric technology is being deployed. Objections to biometrics based on concerns of cleanliness are one of the major issues concerning scanners. Much as with concerns of the cleanliness of public restrooms, participants may feel uncomfortable placing their faces against a machine to have their retinas scanned after many others have done so or touching a hand-geometry scanner during flu and cold season.

Misuse of personal information, including the stealing of identities has become more of a threat. Used in certain ways, biometrics provides greater security because the biometric identifier is much harder to steal or counterfeit. On the other hand, where biometrics are authenticated remotely, that is, by transmission of data from a sensor to a centralized data repository, a hacker might be able to steal, copy, or reverse-engineer

the biometric. This misappropriation could also come about through insider misuse. Without proper safeguards, files could be misappropriated and transactions could be performed using other people's identities.

2. Vein Map Authentication

On the contrary to biometric authentication technology used today, a system which is based on the vein pattern in the palm of a human hand is being developed. The system is essentially a sensor, much like a fingerprint scanner where the user is required to hold their finger over the scanner. However, with this newly developed vein map authentication technology, the user never actually makes contact with the scanner. The sensor can only recognize the vein map if blood is actively flowing the individual's veins. Processing is not affected by race, skin discoloration, hair, age, or time. As veins are internal to the body it is extremely difficult to forge the vein pattern of someone else to gain authentication into the system, thereby enabling a very high level of security. The potential market range is very large due to low cost, high accuracy, response timing, size, and the hygienic and friendly use of the system. The device's way of working will gain public acceptance in the public eye due its contact-less and non-intrusive technology.

The research in this project introduces vein map authentication and tries to persuade the audience of its significance in the biometric world and highlight key points that give vein map authentication an edge over other biometric systems on the market. The author accomplishes this by implementing a rich user interface using the Visual Basic 2005 programming language interacting with Fujitsu's C++ library to control a vein map scanner prototype. The strong capabilities of Visual Studio's CLR's (Common Language Runtime) are used to interact with unmanaged code (code or dlls written outside of the Visual Studio environment). The scope of the project focuses more on the ability of Fujitsu's scanner and API (Application Programming Interface) to extract the vein map pattern from various individuals' palms and the retrieval of the vein map data from a data repository for authentication, as opposed to analyzing the algorithms used for extraction and identification in the C++ library. The user interface consists of a tab control with several tabs containing: group boxes, picture boxes, textboxes, and buttons and labels, each displaying a different function of the software system. The first tab is used for registration of the vein map data. The registration process is necessary to introduce the vein data into the vein map system for comparison during the authentication process. The second tab is used for authentication. This process extracts the vein map of the individual whose palm is over the scanner and compares the extracted vein map to registered data in the vein map repository. The third tab is used as a control system which will authenticate a subject and either unlock a door latch or sound a failure signal. This function of the application is identical to the authentication tab page; however, if the person's vein map is found in the data repository the PC will apply voltage to a USB digital I/O device. A separate function in the application will monitor the I/O device for changing occurrences in voltage and send current through a terminal strip to an electronic door latch, thus locking and unlocking the door.

3. System Design

The vein map authentication software application requires a number of dynamically linked library files owned by Fujitsu Corporation [6]. These DLLs are called from a Visual Basic 2005 project to control a prototype of the vein map scanner also provided by Fujitsu Corporation. For the purposes of the demonstration in this project, there is no licensing needed to use the scanner provided by Fujitsu Corporation. The project is written using the latest version of Microsoft's Visual Basic release; therefore the production machine requires Visual Studio 2005 Enterprise Edition to be installed on it. After the vein map pattern is extracted from the palm, the DLLs return an array of bytes un-encrypted. The application then encrypts the returned data using one of the encryption classes within Visual Studio environment. The encrypted data is then stored in a Microsoft SQL Server database. Therefore, SQL Server 2000 or SQL Server 2005 is required to be installed on the production machine. The application also requires a PC camera for a facial snapshot during registration. The camera must be installed with all its drivers for the application to make use of the imaging device. See Figure 3.1 for a diagram of the system architecture. Text marked in red indicates software and hardware provided by Fujitsu.

The project's solution result produces an executable file (.exe) that controls and calls the Fujitsu scanner and DLLs. For any other machine to run the application besides the production machine, the following are required: Microsoft's .Net Framework 2.0 redistributable package, all Fujitsu DLLs installed and registered within the PC registry, the Fujitsu scanner, an imaging device such as a PC camera, and

depending on if the application will be run in standalone or client/server mode, the machine also needs to have a version of SQL Server installed for the storage of the vein map data. Since the application is to demonstrate how Visual Studio 2005 interacts with the Fujitsu API, the application only requires one table which belongs to the database named VeinMap.

At application startup, the operator starts by entering the person's demographic information that is registered into the system. This information includes the person's full name, date of birth, social security number, ethnicity, hand, and sex. The application then accepts a facial snapshot stored with the demographic information and the vein map data.

During authentication, the person's vein map is taken as input into the system, after the vein map is extracted and stored in memory, each row in the database containing registered vein maps are decrypted and compared until either a match is found or the end of the registration data are queried. At that point, the system either presents the person's demographic information along with their facial snapshot if the vein map of the person being authenticated found a match in the database; otherwise a message appears stating that authentication failed.

3.1. Fujitsu Vein Map Scanner

The Fujitsu scanner works by capturing a person's vein pattern image while radiating it with near infrared rays. The deoxidized hemoglobin in the palm vein absorbs these rays, thereby reducing the reflection rate and causing the veins to appear as a black pattern as shown in Figure 3.2. The vein pattern is then verified against a pre-registered pattern to authenticate an individual. Fujitsu's proprietary algorithm takes into account identifying features such as the number of veins, their position, and the points in which they cross. Internal research by Fujitsu resulted in a false acceptance rate of less than 0.00007% and a false rejection rate of only 0.00004%. False acceptance rate is a rate at which someone other than the actual person is falsely recognized. False rejection rate is a rate at which the actual person is not recognized accurately. [6]

4. Testing and Evaluation

Testing was conducted before, during, and after the software in the project was developed. A number of software testing strategies are proposed in the literature. The strategies followed include, technical review by someone other than the author of the project, testing at the component level working outwards, using Microsoft Visual Studio's rich debugger, and most of all experience and intuition. Unit testing focused on the smallest unit of the software design, each component that the application was constructed upon, and the modules that the applications were built from. Each of the four classes that are used in the application where first developed as stand alone programs and rigorously tested before being integrated into the overall product. Figure 3.3 and figure 3.4 show some of the classes as a standalone application.

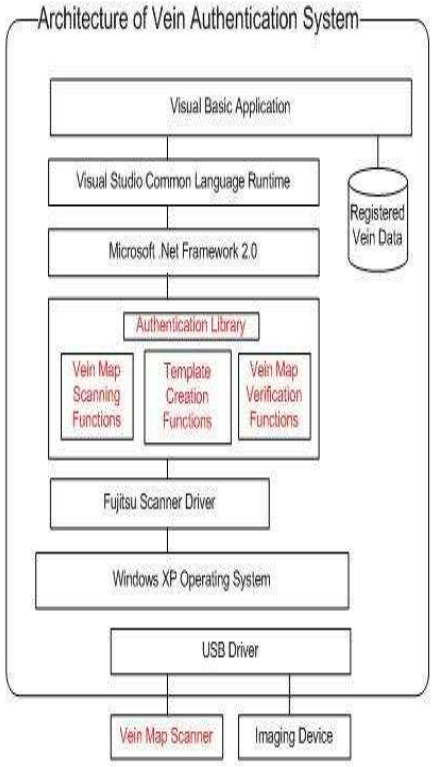

Figure 3.1 System Architecture

Using the component level design description as a guide, the most important control paths were tested using white-box and black-box testing techniques to uncover errors within the boundary of each module. Class FVM.vb itself was not tested at the component level since the class is solely responsible for marshalling all memory and declaring all enumerations and structures that interact with the vein map scanner; its purpose functions as a header file in c++. Its components were tested during integration testing. Each of the components in iCam.vb were tested with its

standalone application, all the components in the class CopyFrame, SetCam, SetFrameRate, InitCam, and CloseCam are equally important. Each components has two control paths, if…, else…, and were forced to execute at each level. VMA.vb was the most critical class to test at the component level since its purpose is to dynamically allocate memory at runtime based on the number of vein map templates there are in the data repository. The snippet of code is adding the vein map data to a temporary 2-D array for comparison. Like the FVM.vb class the SEAIO.vb class was not tested at the componet level in that its sole purpose is a wrapper (header) file that has the function definitions to inteact with the SEALEVEL Corporation API that control their I/O device.

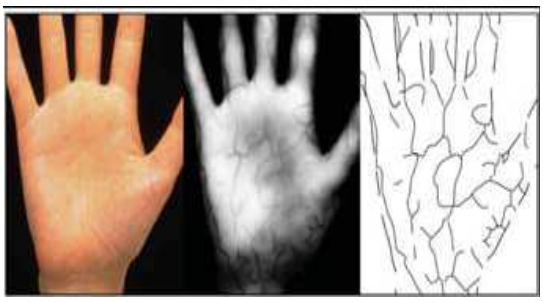

Figure 3.2 Vein Map after near infrared light Penetration [6]

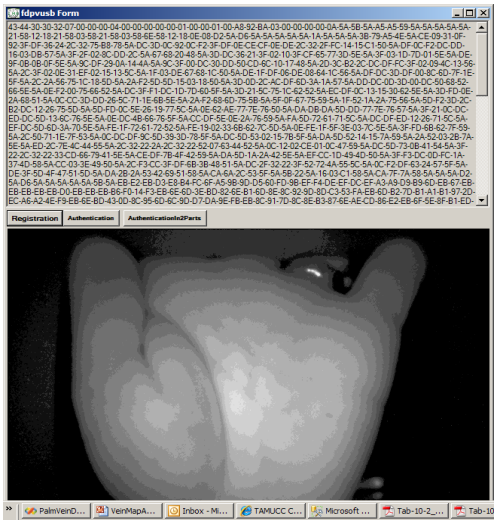

Figure 3.3 FVM class as standalone application

The complexity of each test and the errors that those tests uncovered were limited by the constrained scope established for each unit test. Each unit test focused on the internal processing logic and the data structures within each component. Integration testing focused on putting all the modules and components together, each class was added and tested to the driving module, frmPalmVeiw.vb, before any other was added. After each module was added to the project, instantiation tests were conducted to make sure all classes were instantiated and all structures and enumeration initialized before use. No problems were uncovered. System testing encompassed a series of different tests whose primary purpose was to fully exercise the program. Testing the application and capturing the Task Manages performance report on a Windows XP machine with three quarters of a gigabyte of memory produced the report shown in figure 3.5 and figure 3.6.

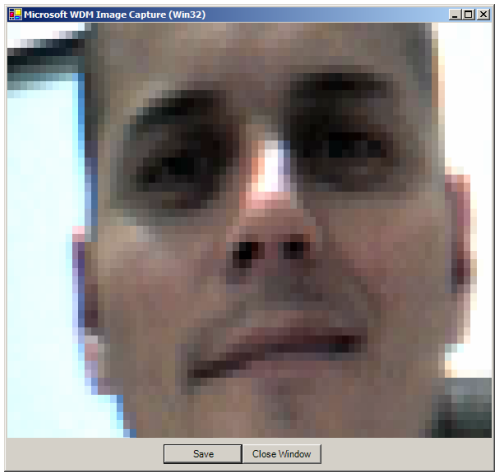

Figure 3.4 iCam class as standalone application [11]

The same frame was taken of Task Manager's performance report during authentication on a Windows Vista operating system with 1.1 gigabytes of memory. These tests ensured that error-handling paths are designed for all information coming from different elements of the system and that bad data or other potential errors in the software were uncovered. Recovery testing ensured that the application handled and recovered from faults in a timely manner. The system was forced to fail in different ways. For example during runtime, a specific device was disconnected intentionally from the workstation causing the application to crash and produce a specific error. Code was added to the application to reinitialize itself before being used again. Also, a specific encrypted column in the database was manually tampered with to ensure that decryption could not take

place if the data were modified outside the application. In this case the application did not recover and that cell in the data repository was corrupt unless changed to its original state.

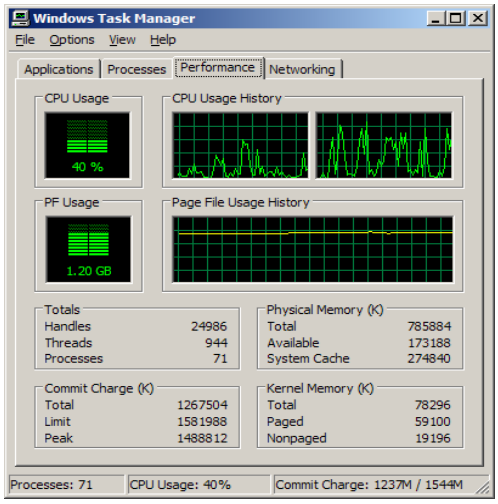

Figure 3.5 Windows XP Performance Report during Authentication

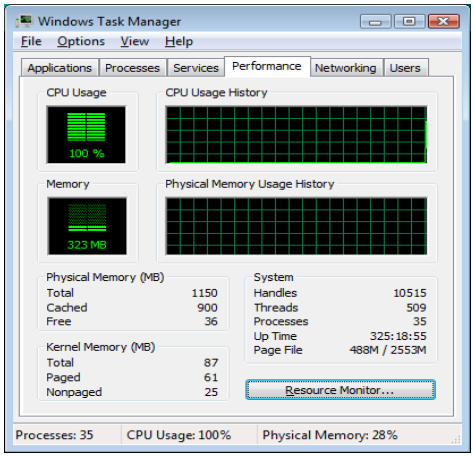

Figure 3.6 Windows Vista Performance Report during Authentication

Security testing ensured that protection mechanisms built into the system protected the application from improper penetration. The system is very secure and robust. All the vein map data previously registered are stored in a SQL Server 2005 database which is password protected to gain access. The data within the repository are symmetrically encrypted using the RijndaelManaged crytocraphy class provided by Visaul Studio, a salt value is read from an application configuratin file, and an MD5 hash of the ResgistrationId is used as a private key. Seganography was considered as a mechanism to hide the private key, but opted agianst due to image distortion

5. Conclusion

There are various authentication systems out on the market today, however all have been found to have flaws or are not widely accepted by society. Throughout this research, vein map technology is introduced as a robust authentication system for today's security need. Proper design and implementation of the proposed authentication system is the cornerstone to its security. The software created in conjunction with this project is intended to solely introduce the committee to vein map authentication and programming using the Visual Studio 2005 environment. Continued work using vein map technology should include, research and possible development of the algorithm or algorithms used to extract the vein map from the palm and implementation of sending the authentication data via IP, e.g., the data repository could be located in Langley, Virginia, while the person under authentication could be in Baghdad, Iraq. There are various USB over IP devices on the market today which could make this possible.

6. References

[1] ACLU 2002. Flaws in Face-Recognition at Palm Beach Airport**,** available from http://www.aclu.org/privacy /spying/1486 4prs20020514.html (visited October 9, 2006)

[2] Biometrics Insight 2006. What is Biometrics? Available from http://www.biometricinsight.com/biometrics.html (visited, September 28, 2006)

[3] **D.** Bolme, M. Teixeira, and B. Draper. ***The CSU Face Identification Evaluation System: Its Purpose, Features and Structure,*** International Conference on Vision Systems.(April 1-3, 2003) 304-311.

[4] J. Daugman. University of Cambridge: Computer Laboratory: Webpage for John Daugman. Image available from http://www.cl.cam.ac.uk/users/jgd1000/ (visited October 7, 2006)

[5] findBiometrics 2006 Feature Article Archive. Available from http://www.findbiometrics.com/Pages/feature_ archive.html (visited October 9, 2006)

[6] Fujitsu 2006. PalmSecure: Palm Vein Authentication System http://www.fujitsu.com/us/services/biometrics/palm-vein/#footnote0 (visited October 29, 2006)

[7] M. Hill. The University of New South Wales, ANAT2310: Eye Development. Available from http://anatomy.med.unsw.edu.au/cbl/teach/anat2310/Lecture06Senses(print).pdf (viewed October 8, 2006)

[8] International Biometric Group, 2006 Image available from http://www.biometricgroup.com (visited October 5, 2006)

[9] J. Lu. Boosting Linear Discriminant Analysis for Facial Recognition

[10] J. Lu. Plataniotis, K.N.m and Venetsanopoulos, A.N. *Regularized Discriminant Analysis for the Small Sample Size Problem in Face Recognition*, Pattern Recognition Letters, (December 2003), Vol. 24, Issue 16: 3079-3087

[11] MIT Media Laboratory 2002. Photobook/Eigenfaces Demo, Image available from http://vismod.media.mit.edu/vismod/demos/facerec/basic.html (visited October 9, 2006)

[12] Outlaw.com 2002. Masons, P. Major flaws in biometric security products. Available from http://www.out-law.com/page-2624 (visited October 2, 2006)

[13] SecuGen Biometric Solutions, 2004. Image available from http://www.secugen.com/images/faq02.gif (visited October 5, 2006)

[14] L. Sirovich. and M. Kirby. *A Low-Dimensional Procedure for the Characterization of Human Faces*, J. Optical Soc. Am. A (1987) Vol. 4, No.3, 519-524.

[15] Technovolgy.com 2006. Unknown. Biometric authentication: what method works best? Available from http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16 (visited October 1, 2006)

[16] University of Arkansas for Medical Science. Information for Patients: Retina Services - Age-Related Macular Degeneration. Image available from http://www.uams.edu/jei/patients/retina_services/maculardegen.asp (visited October 7, 2006)

[17] VideoSurveillanceGuide 2006. Osborn, A. Biometrics history - looking at biometric technologies from the past to the present. Available from http://www.video-surveillance-guide.com/biometrics-history.htm (visited September 26, 2006)

[18] B.Westmoreland., M. Lemp, and R. Snell. *Clinical Anotomy of the Eye 2nd ed*. Blackwell Science Inc., Oxford 1998

[19] L. Wiskott,. Face Recognition by Elastic Bunch Graph Matching, available from http://www.neuroinformatik.ruhr-uni-bochum.de/ini/VDM/research/computerVision/graphMatching/identification/faceRecognition/contents.html (visited October 9, 2006)

[20] Wikipedia 2006. Wikipedia the free Encyclopedia: The Stone Age http://en.wikipedia.org/wiki/Stoneage (visited October 16, 2006)