RESEARCH AND DEVELOPMENT OF AN IRIS-BASED RECOGNITION SYSTEM FOR IDENTIFICATION AND SECURE AUTHENTICATION

Hussein H. FAKHRY and Benedict Bernard CARDOZO

Abstract: New developments in Iris recognition technology provide increased potential for security. The research study described in this article has been conducted to further explore its potential through the development and evaluation of a working prototype system for Iris Administration and Organization Resource Access Control. The developed prototype possesses Iris administration functionality with such functions as enrollment, identification, verification, update and deletion. Also, the prototype organization module allows management of organizational resources access control. Testing of the prototype has been performed at the Dubai Naturalization and Residency Department (DNRD) site. The test has demonstrated the usefulness of Iris authentication for automating passport control. Special Application Programming Interface (API) licensed from Iridian Technologies has been used in this development.

Keywords: Iris Recognition, Biometric, Security Access, Iris Authentication.

Introduction

Iris recognition is a biometric technology for identifying humans by capturing and analyzing the unique patterns of the iris in the human eye.[1] Iris recognition can be used in a wide range of applications in which a person's identity must be established or confirmed. For example, these include passport control, border control, frequent flyer service, premises entry, access to privileged information, computer login or any other transaction in which personal identification and authentication relies on knowledge-based or token-based passwords. Nevertheless, one of the most dangerous security threats in today's world is impersonation, in which somebody claims to be someone else. Through impersonation, a high-risk security area can be vulnerable. An unauthorized person may get access to confidential data or important documents can be stolen. Normally, impersonation is tackled by identification and secure authentica-

© ProCon Ltd. This article cannot be reprinted, published on-line or sold without written permission by ProCon.

tion, however, the traditional—knowledge-based (password) or possession-based (ID, Smart card)—methods are not sufficient since they can be easily hacked or compromised. Hence, there is an essential need for personal characteristics-based (biometric) identification due to the fact that it can provide the highest protection against impersonation. Among other biometric approaches, the new Iris recognition technology promises higher prospects of security.[2] Therefore, this research is conducted to further explore the potential of the Iris recognition technology and to demonstrate its potential through the development and evaluation of a working prototype.

Problem Definition

This research study explores the Iris recognition technology and develops a working prototype for an important application area – the Dubai Naturalization and Residency Department (DNRD), Dubai, United Arab Emirates. The application under consideration has a number of sensitive security issues, which could motivate the management of DNRD to implement the Iris recognition technology. A brief overview of DNRD and its basic activities is given in order to provide a better understanding of the issues.

History of Iris Recognition

The Iris recognition technology captures and analyzes the unique features of the iris in the human eye to perform identification. The algorithms recognizing persons by Iris recognition are very accurate to the extent that the entire planet can be enrolled in an Iris database with very little possibility of false acceptance or false rejection.[3] The first claim that no two irises are identical was made by Dr. Leonard Flom and Dr. Aran Safir, both ophthalmologists, in mid 1980s.[4] The claim was based on their clinical research that every iris is different and was seen to remain unchanged in clinical photographs. This claim made the human iris as a good candidate for a biometric solution and after substantial research the patent of using iris as a means for identifying persons was awarded to them in 1987.[5] Later in 1989, Dr. John Daugman developed algorithms for recognizing persons by iris recognition. The algorithms were patented in 1994 and nowadays they form the basis of all current iris recognition systems and products.[6]

Iris Characteristics

The human iris is a colored oval- to round-shaped ring surrounding the pupil of the eye. Figure 1 shows a sample iris.[7] It consists of muscles that adjust the size of the pupil. The iris is the only internal body organ that is visible externally. One of the most distinctive characteristics is its stability. The iris pattern stabilizes by the second

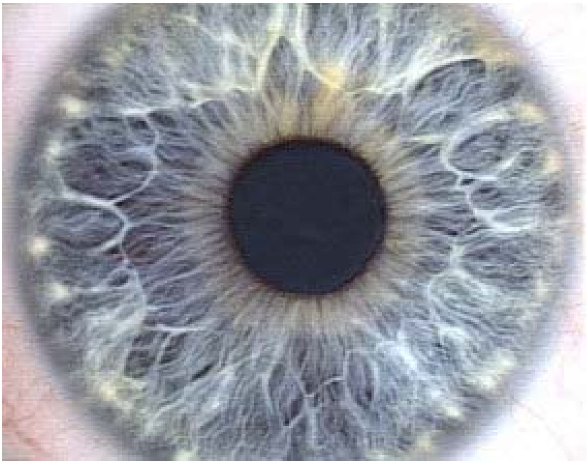


Figure 1: The Human Iris.[8]

year of birth and remains unchanged throughout person’s lifetime unless injured or damaged by accident or disease.

The complex pattern of the iris contains many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette [9] that differentiate one iris from another. One of the major primary visible characteristic is the trabecular meshwork tissue, which gives the appearance of dividing the iris in a radial fashion.[10] This meshwork is formed permanently by the eighth month of gestation. Another important factor is that during development of iris there is no genetic influence on it, which is proved by a process known as “chaotic morphogenesis” occurring at seventh month of gestation. This means that even identical twins have completely different irises. As the iris is small in radius (about 11mm), it is a problem to get an image. However, it has great mathematical advantage because its pattern variability among different persons is very large.[11] This is due to the fact that the iris has more than 266 degrees of freedom,[12] which is the number of variables in the iris pattern that allow it to differ from another iris.

Other iris characteristics that make it appealing for authentication are:[13]

- The iris pattern is more complex and more random than other biometric patterns and hence offers a highly precise method for individual authentication with a false acceptance error rate of less than one in two million records.
- The iris located in the human eye is protected behind the eyelid, cornea and aqueous. This helps it to keep the damage and abrasion minimal. In addition, it is nearly impossible to forge identity.

- The iris pattern remains stable and unchanged after the age of two years and does not degrade over time or with the environment.
- The probability of two irises producing the same numerical code is almost zero.
- A distinctive iris pattern is not susceptible to theft, loss or compromise.
- Each iris is different, even between identical twins or between left and right iris of an individual.
- Since the iris is an extremely complex structure, modification of the iris would require sophisticated intricate microsurgery. This could result in individual loss of sight or an obvious artificiality that can be easily seen visually or through image analysis.

Physical Access Systems

This section describes some of the widely used commercial applications using the iris recognition technology for controlling and monitoring physical secure access to restricted areas and resources.

IrisAccess® 2200T System

Iridian Technologies and LG Electronics have teamed up together to create the IrisAccess® 2200T system.[14] The system is used to identify and authenticate user access to physical areas. The system designed and developed using Iridian Technologies' Iris recognition software and LG's imaging platforms delivers superb accuracy, speed, scalability and convenience for user identification and authentication. Some of the features of the IrisAccess® 2200T system are summarized below.

The imaging device automatically detects that a subject is approaching. The individual has to glance at the imaging device from a distance of 3–10 inches, which captures the iris image and digitally processes it to form a 512 byte IrisCode® template.

A patented search function enables real time database matching at remote unit level. User access is granted immediately as soon as the presented IrisCode® matches a valid IrisCode® template in the database.

Using organization Intranet and encrypted transaction, TCP/IP communication, the system can control the access to the secure area within the organization and up to 254 doors over the Internet.

Other features include audio interface in multiple languages, non-intrusive, one to many search identification and optional verification mode.

EyePass™ System

The EyePass™ System developed by EyeTicket Corporation [15] is primarily aimed at aviation industry. It is an access control service provided to air carriers, airport authorities and other large employers. Some of the features of the EyePass™ system are:

- Access control to secure areas for pilots, flight crews and ground staff at airports and corporate installations.
- Time and attendance functions are automated and secured by the system.

JetStream™ System

The JetStream™ System also developed by EyeTicket Corporation is used for positively identifying and authenticating passengers traveling on airlines. It is used in conjunction with the airlines' reservation system. Some of the features of the JetStream™ system [16] are: (1) Simplifies and expedites transactions providing maximum security and risk management at a competitive cost; (2) Allows passengers' to check in and board an aircraft simply by using one's iris. The JetStream™ system is a fully developed proven solution currently deployed at London Heathrow Airport.[17] Other application areas using the JetStream™ system include immigration control, railways and hotel industry.

Information Security

This section describes a commercially available application based on the iris recognition technology that addresses the issues of password management and uses one's iris as a positive identity to authenticate the access to data and information.

Panasonic Authenticam™

Iridian Technologies and Panasonic have teamed up to design and develop a system that primarily addresses issues related to passwords, PINs and token cards. Panasonic's Authenticam™ (see Figure 2) enabled with unique PrivateId™ software from Iridian Technologies allows the iris recognition camera to capture, select and secure iris images.[18] Some of the important features of the system are summarized below.

Panasonic's Authenticam™ enables system administrators to secure access to personal computers, files, folders, and applications only to authorized users. It uses the PrivateID™ software, which generates IrisCode® compatible with KnoWho™ Authentication Server from Iridian Technologies. Also, it includes the I/O software SecureSuite™, which allows multiple users to securely access restricted resources. The cost associated with password management and the risks of fraudulent activities are substantially reduced.

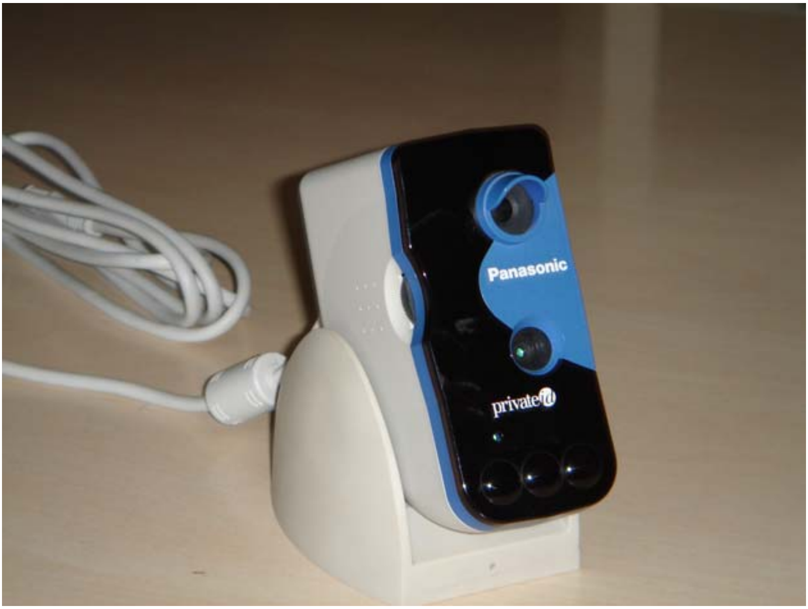


Figure 2: Panasonic's Authenticam™ Enabled with Private Id™ Software.

Authentication Server

The KnoWho™ Authentication Server from Iridian Technologies is designed to integrate with mission critical applications, transaction systems, network environments that require high performance authentication capabilities.[19] The authentication server is a major component used to store IrisCode® templates and to process the authentication. The Authentication server has two main functions, first to store IrisCode® templates and second – a processing engine that performs real-time matching. The KnoWho™ Software Development Kit (SDK) allows customization of the Authentication server capabilities for other applications. Some of the features of the KnoWho™ Authentication Server are [20]:

- Identification/ Recognition: one-to-many matching.
- Verification: one-to-one matching.
- Ability to enroll, update and delete new and existing IrisCode® templates, data etc.
- Use of Oracle 8i and SQL Server RDBMS to store IrisCode® and related data.
- Compatible with PrivateID™ supported cameras such as Panasonic Authenticam™.

- Data encryption at database level.
- Option to store facial images.

System Development Approach

Three approaches to system development have been considered and compared, namely the System Development Life Cycle (SDLC), the Object-Oriented Development (OOD), and the Rapid Application Development (RAD).

However, the RAD approach has been preferred for the following reasons:

- The main components and functions of the proposed system such as iris enrollment, recognition, verification and deletion are implemented using the pre-existing class libraries (API) licensed from Iridian Technologies. Hence, the RAD approach is suitable for fast development of the remaining components of the proposed system.
- Using RAD, the development of the system can be accelerated so as to prove and demonstrate to the management of DNRD as well as to other interested organizations the benefits of using a superior biometric technology to achieve a competitive advantage in solving their security problems.
- Through RAD, the project requires fewer resources and less time to rollout the final product resulting in reduced project costs.
- The final product is aimed at highly specialized information systems market and its distribution will be focused at in-house market for example at industries or at government establishments and quick development of the system can only make this possible.
- Using RAD helps in combating scope and requirements creep by limiting the project exposure to change – since changes are very much inevitable in long development processes such as in the System Development Life Cycle (SDLC) and the Object-Oriented Development (OOD) approaches, which can lead to significant expenses and waste of time and effort for redesigning and redevelopment.

Therefore, the RAD approach has been used to efficiently develop a reliable and robust prototype system while taking into consideration the continuous feedback from higher management executives, analysts and users.

Features of the Proposed System

The development of the proposed Iris Administration and Organization Resource Access Control System (illustrated in Figures 3 and 4) required development of four different modules which are:

1. Iris Administration.
2. Organization Resource Access Control Management.
3. Authentication and Secure Access to a protected resource using one’s iris.
4. Link and Automate passport control for DNRD. It links the newly captured iris with DNRD’s existing customer record in the database and automates Passport Control at Dubai International Airport.

The possible features of each module are summarized below.

1. *Iris Administration*

- Enrollment: The system should capture left, right and face images of a subject as well as his/her personal details and include/register the person in the biometric and application databases, respectively.
- Recognition: The system should retrieve all details of the person including iris and face images when one’s iris is provided for identification.
- Verification: The system should verify the person by comparing the data and iris provided.
- Update: The system has to provide modification of personal data.
- Deletion: The system should permit, when needed, deletion of all personal data and the relevant biometric data from the application and biometric databases, respectively.

2. *Organization Resource Access Control Management*

The system allows adding and deleting resources from the organization hierarchy tree; however, in the presented research, the organizational resources are pre-defined.

The system retrieves the details of the enrolled person based on some criteria such as name, personal identification number, etc. Using the retrieved data, the system grants access to a resource for a single or many persons. Using the retrieved data, the system might also revoke access to a resource for a single or many persons. The system displays the granted resources for a person.

3. *Authentication and Secure Access*

The system should be able to grant access to a protected resource. The protected resource simulated for this particular project is the information data main menu that is given access to by using one’s iris or optionally by entering user login name and password. The organizational resources access control module manages the access to the main menu options. In case of a failure of the biometric system, the system should permit to the user access to the protected resource by using his/her login name and

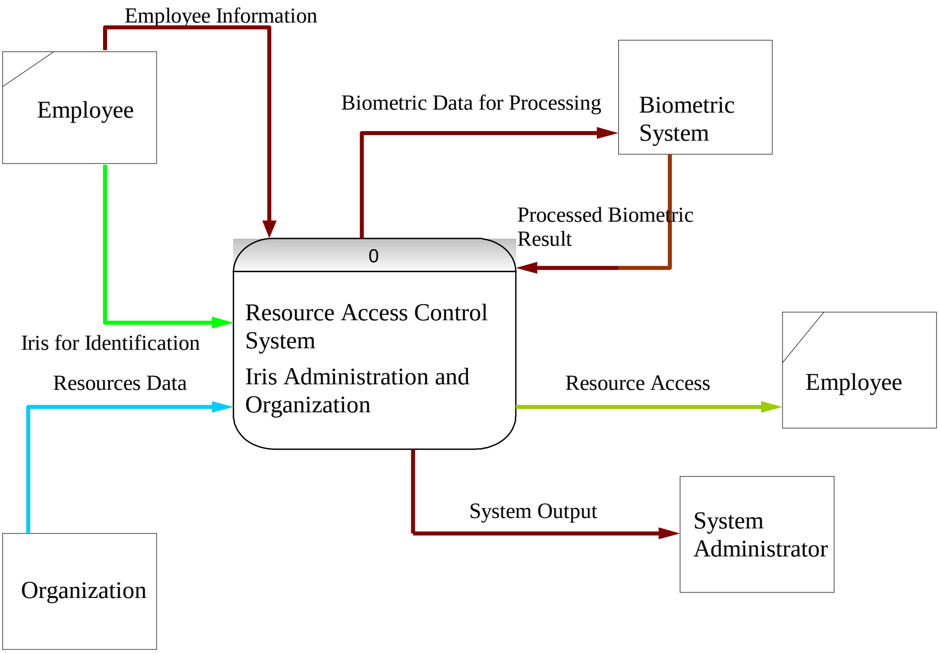


Figure 3: Context Diagram of the Proposed System.

password. Only the menu options that are granted access to should be enabled, whereas others should be disabled.

4. *Link and Automate Passport Control for DNRD*

The system will use the existing program module from DNRD to link its customer database with the enrolled person. The customer could expedite his/her passport and immigration checks by providing his iris – the system will automatically make an entry or output record for the person in the DNRD database.

Development Environment

The development environment consists of the technologies, programming languages, standards, protocols and tools that are used in developing the Iris Administration and Organization Resource Access Control System. The major components used for building the prototype system described in this article are the PrivateID™ and KnoWho™ Authentication Server APIs from Iridian Technologies. The other components in the development environment are ActiveX control developed using Microsoft Visual C++, Form Builder v6 in Oracle Developer 2000 environment and

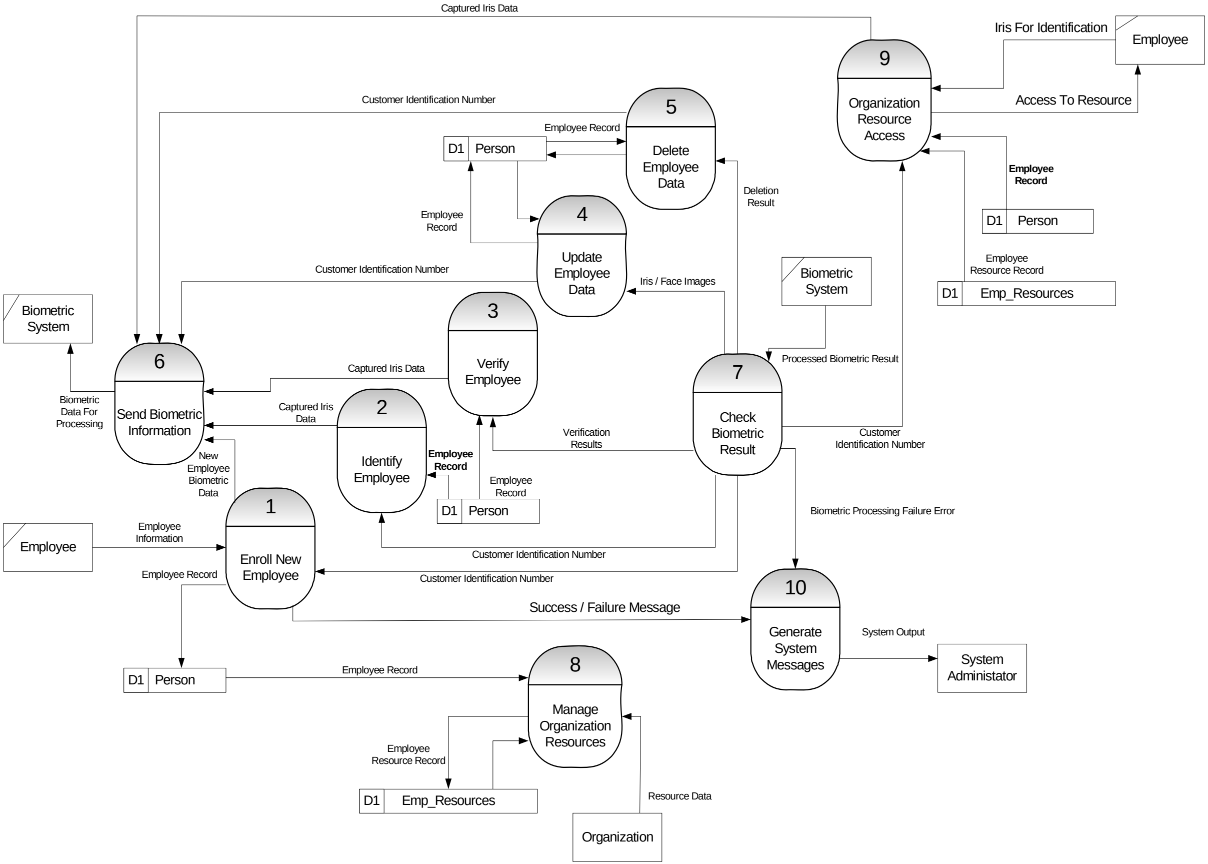


Figure 4: Level 0 Data Flow Diagram of the Proposed System.

Oracle 8i Relational Database Management System (RDBMS). Figure 5 illustrates the system components, highlighting the components developed in this study.

PrivateID™ and KnoWho™ Authentication Server

PrivateID™ and KnoWho™ Authentication Server can be integrated into new or existing systems. The open architecture of both PrivateID™ and KnoWho™ Authentication Server makes it possible to integrate the iris recognition technology into distributed applications such as Internet applications.

It also makes the network security solutions easy to implement.

The basic components include:

1. PrivateID™ software – image capturing software that runs on clients' computers.
2. PrivateID™ enabled video camera such as Panasonic Authenticam™ with specialized lens for photographing the iris.
3. KnoWho™ Authentication Server – a highly secure and scalable transaction server.
4. Biometric Database – a RDBMS such as Oracle or SQL Server maintained exclusively by the KnoWho™ Authentication server.

A typical client-server application using PrivateID™ and KnoWho™ Authentication Server performs the following steps:

- The application running on the client side requests the PrivateID™-enabled video camera such as Panasonic Authenticam™ to capture an iris image of the subject.
- The PrivateID™ software would return the captured iris data to the calling application code.
- The application running on the client side would send the data to the server side of the application that calls the KnoWho™ Authentication Server API to perform biometric processing (e.g. perform recognition).
- The KnoWho™ Authentication Server would return a result to the calling application.
- Based on the result, the application would decide whether to grant or reject access to the protected resource.

PrivateID™ software

The PrivateID™ software allows an iris recognition enabled camera such as the Panasonic Authenticam™ to capture, select and secure iris images. The software was

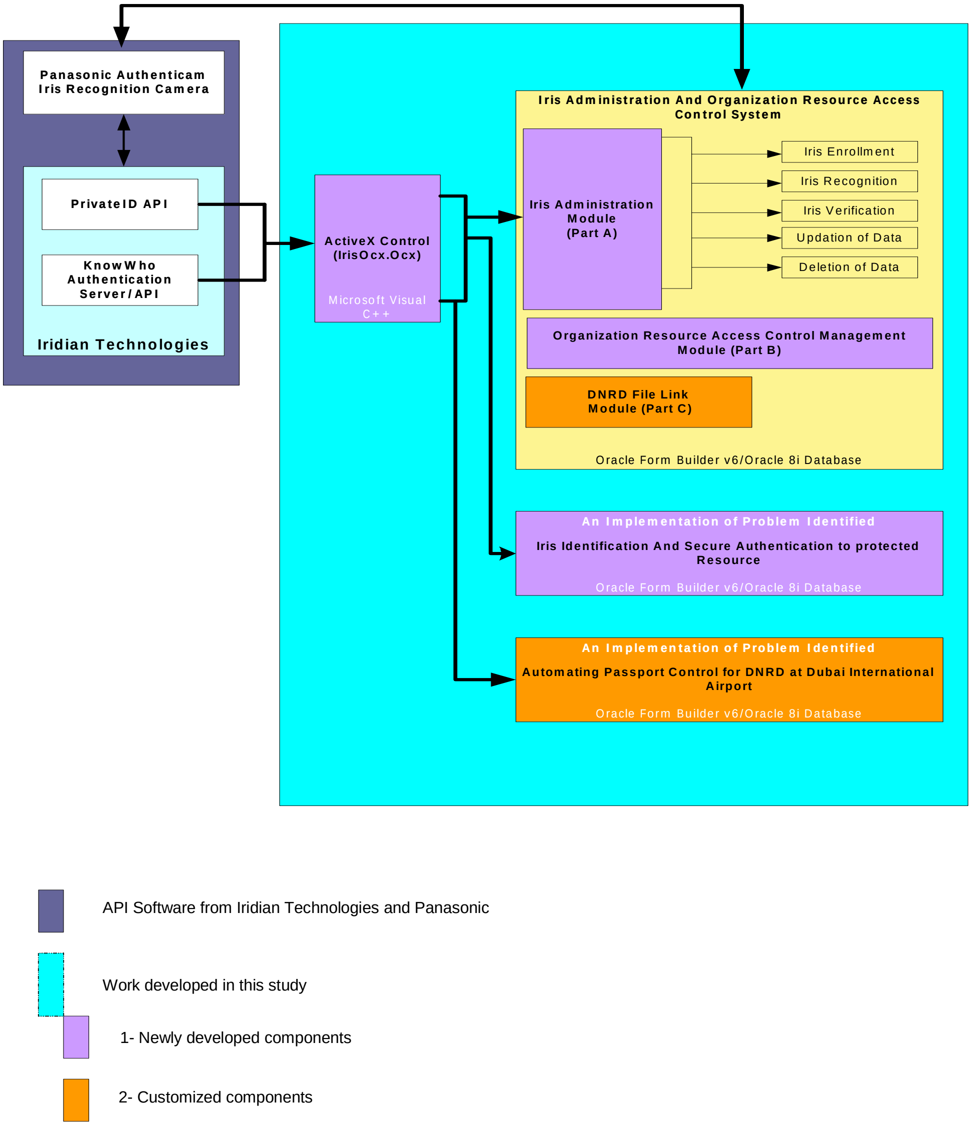

Panasonic Authenticam Iris Recognition Camera
PrivateID API
KnowWho Authentication Server/API
Iridian Technologies
ActiveX Control (IrisOcx.Ocx)
Microsoft Visual C++
Iris Administration And Organization Resource Access Control System
Iris Administration Module (Part A)
Iris Enrollment
Iris Recognition
Iris Verification
Updation of Data
Deletion of Data
Organization Resource Access Control Management Module (Part B)
DNRD File Link Module (Part C)
Oracle Form Builder v6/Oracle 8i Database
An Implementation of Problem Identified
Iris Identification And Secure Authentication to protected Resource
Oracle Form Builder v6/Oracle 8i Database
An Implementation of Problem Identified
Automating Passport Control for DNRD at Dubai International Airport
Oracle Form Builder v6/Oracle 8i Database
API Software from Iridian Technologies and Panasonic
Work developed in this study
1- Newly developed components
2- Customized components

Figure 5: Components of the Developed System.

basically designed for information management and security. The only important function is capturing and selecting iris images for transfer and further processing for authentication.[21] The software captures a series of video digital images of the individuals' eye. The iris image is inspected for sufficient quality and content using built-in image quality metrics within the software.[22] This ensures that the image provided to the server will have high confidence levels for a successful match outcome. The software also provides an audible beep just like the "closing of camera shutter" to inform the user that the image capture session is complete. A configurable timeout parameter can also be set for iris image capture session during which time if an image of high quality is not obtained, the whole process has to be repeated again. The image provided by PrivateID™ is in a compressed format. PrivateID™ and KnoWho™ Authentication Server work in single-factor authentication mode, requiring no other information in association with the record.[23] A nonce is used by the PrivateID software to prevent replay of transactions by a hacker or a third party software tool. A nonce is defined as an item that is used once and discarded.[24]

A nonce is a randomly generated number of 16 bytes that is concatenated to the iris image before it is encoded using either Blowfish or 3DES encryption methodologies. For the implementation of this project, 3DES encryption has been used. The encoded iris image with message authentication code (MAC) is sent to the authentication server. The authentication server uses its active 3DES private key to decode the iris image with MAC to continue with further processing.

Using such a technique, the Iris image becomes used one and discarded data package. Replay cannot be performed because the original nonce does not match any of the active nonces on the server either because it has expired, timed out or is not valid due to used-only-once policy.

PrivateID™ Application Programming Interface v2.1

The PrivateID™ Application Programming Interface (API) provides functions or interfaces that enable video capturing of the iris or the face.[25]

The CLCaptureIrisNonce function captures an iris image of suitable quality that will be sent to the KnoWho™ Authentication Server for biometric processing. This function is used with the nonce described in the previous section.

KnoWho™ Authentication Server

The KnoWho™ Authentication Server accepts the iris image sent via PrivateID™-enabled iris recognition camera, checks for image integrity and then performs the biometric processing requested by the client application, for example verification (1:1 matching) or identification (1:many matching). After validating the integrity of incoming data, it then creates an IrisCode template for matching the IrisCode templates that already exist in the system.[26] The KnoWho™ Authentication Server supports five main operations that include enrollment, verification, recognition, update and deletion. The KnoWho™ Authentication Server stores three types of biometric information, which are as follows:

- IrisCode templates (left or right eye or both) stored in cache and on disk.
- Iris images (left or right eye or both) on disk.
- Portrait facial images (JPEG format, about 20 KB) on disk. The KnoWho™ Authentication Server stores only the individual identification number indexed with the IrisCode template. No personal data is stored, thereby ensuring privacy. Figure 4 depicts the individual privacy at KnoWho™ Authentication Server.

Passport Control Automation for DNRD

To automate the passport control process, two programs from DNRD were customized so as to link to the Iris Administration and Organization Resource Access Control System. In an all person inquiry program from DNRD, the employee data was retrieved from the DNRD database and a link was made with the enrolled employee data in the application database. Since the DNRD information is strictly confidential and sensitive, only the DNRD employee's file number was stored in the application database. The other program for passport control embeds the reusable ActiveX control component developed in this project. When the registered employee presents his/her iris, the CIN retrieved from the biometric database links with the PIN from the application database which in turn is linked to DNRD employee's file number. The employee's file number is used to retrieve the details from DNRD and automate the entry – exit transaction. Figure 6 displays the actual development of the system made in the course of this research study.

Testing Plan for the Developed System

Testing of the developed system is performed in two phases: unit testing and integration testing.

Unit Testing

In this phase, the ActiveX control component was tested for the following conditions using the ActiveX control test container available in Microsoft Visual Studio:

- Connectivity to KnoWho™ Authentication Server. To perform iris administration tasks, the ActiveX control component must be able to connect to the authentication server. The ActiveX component method 'GetServer-Status' is invoked to check the connectivity to the server.

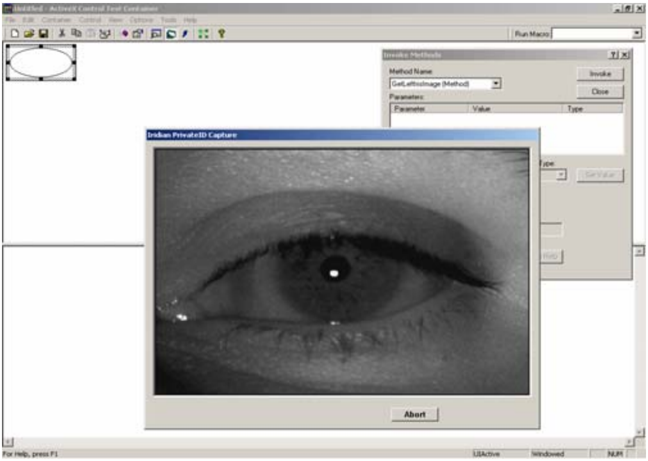

Untitled - ActiveX Control Test Container
File Edit Container Control View Options Tools Help
Run Macro
Invoke Methods
Method Name
GetLeftIrisImage (Method)
Invoke
Close
Parameters
Parameter
Value
Type
Type
Set Value
Help
Iridian PrivateID Capture
Abort
For Help, press F1
UIActive
Windowed
NUM

Figure 6: ActiveX Control Unit Testing for Left Iris Capture.

- Capturing of iris images. Another very important functionality of the ActiveX control is to capture iris images for the purpose of enrollment, identification and verification. Two methods are available for this purpose: GetLeftIrisImage and GetRightIrisImage. Figure 6 shows the PrivateID™ iris capture window when the method GetLeftIrisImage is invoked. The function returns zero if the capturing of the iris image is successful.

All remaining functions or methods of the ActiveX components were tested prior to integrating them with the application.

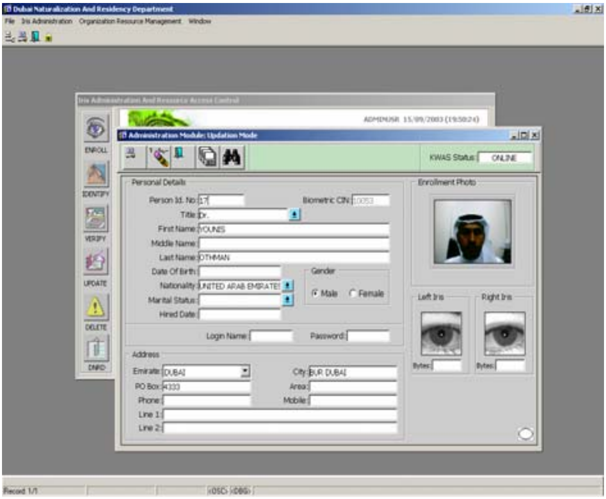
Integration Testing

Integration testing involves building the whole system using the final set of completely-tested individual program components and testing the resultant system for problems that may arise from interactions between the components.[27] To minimize errors and to find the source of error quickly, the incremental approach of adding and testing components is usually followed. The benefits of the incremental integration approach are:

- Errors can be found easily when the number of integrated components is small. This helps in locating and resolving the source of error quickly.
- A new component will be added only if the system with the existing components is completely error-free. In case of a new error, it can be easily attributed to the last added component.

The disadvantage of integration testing is that testing a system feature may require more than one component at a time to be integrated. Testing may find errors between individual components and other parts of the system.[28] Due to this fact, fixing errors can be difficult since it may affect the system functionality as all the components may change. Furthermore, introducing a new component may result in interaction error with previously integrated tested component.

Figure 7 illustrates how a staff member of the Information Technology section at DNRD tests the Iris administration and Organization Resource Access Control System.



Dubai Naturalization And Residency Department

Iris Administration And Resource Access Control

ADMINUSR 15/09/2003 (19:50:24)

Administration Module: Updation Mode

KWAS Status: ONLINE

Personal Details

Person Id. No: 17

Biometric CIN: 10053

Title: Dr.

First Name: YOUNIS

Middle Name:

Last Name: OTHMAN

Date Of Birth:

Nationality: UNITED ARAB EMIRATES

Marital Status:

Hired Date:

Gender: ● Male ○ Female

Login Name:

Password:

Address

Emirate: DUBAI

City: BUR DUBAI

PO Box: 4333

Area:

Phone:

Mobile:

Line 1:

Line 2:

Enrollment Photo

Left Iris

Bytes:

Right Iris

Bytes:

Record 1/1

<OSC> <DBG>

Figure 7: DNRD Staff Testing the System.

Concluding Remarks

The research presented in this article has demonstrated the design, development and implementation of an efficient and reliable prototype using the iris recognition technology that has the potential to bring intangible benefits to organizations wishing to enhance or integrate new security policies for their protected resources. The iris recognition technology is the most accurate, fast and less invasive one compared to other biometric techniques using for example fingerprints, face, retina, hand geometry, voice or signature patterns. The system developed in this study has the potential to play a key role in areas of high-risk security and can enable organizations with means allowing only to the authorized personnel a fast and secure way to gain access to such areas. In particular, the developed system allows:

- Enrolling a person in the biometric system by capturing his/her irises.
- Accurately identifying (1:many search) a person by just capturing any of his/her irises.
- Verifying (1:1 search) a person by matching his/her data linked in the system with one’s iris.
- Access for the enrolled employee to organization’s protected resource by capturing his/her iris.

The Rapid Application Development approach used for design and development has delivered a highly robust and generic product, which can be easily customized for any other organization or industry. Moreover, the reusable ActiveX control component created for this system can be easily deployed in many Windows-based development tools. The presented system has been implemented using Panasonic’s Authenticam™ with the Private ID™ software and the KnoWho™ Authentication Server from Iridian Technologies. To date, these are the only Application Programming Interfaces (API) available on the market. Almost all applications worldwide based on the iris recognition technology have these APIs integrated with them. Iris recognition can be used for physical access security, information data security, border control, automated passport control, banking, services and manufacturing industries. The list with potential application areas is open since iris recognition can serve many other purposes.

Notes:

[1] John G. Daugman, “High Confidence Visual Recognition of Persons by a Test of Statistical Independence,” *IEEE Transactions on Pattern Analysis and Machine Intelligence* 15, no. 11 (November 1993): 1148-1161.

[2] John G. Daugman, “Biometric Personal Identification System Based on Iris Analysis,” U.S. Patent No. 5,291,560 issued March 1, 1994.

[3] John G. Daugman, “The Importance of Being Random: Statistical Principles of Iris Recognition,” *Pattern Recognition* 36, no. 2 (2003): 279-291.

[4] Daugman, “The Importance of Being Random: Statistical Principles of Iris Recognition.”

[5] Daugman, “High Confidence Visual Recognition of Persons by a Test of Statistical Independence.”

[6] Daugman, “Biometric Personal Identification System Based on Iris Analysis.”

[7] John G. Daugman, “Sample Iris Image,” <http://www.cl.cam.ac.uk/users/igd1000/sampleiris.jpg> (15 May 2003).

[8] Daugman, “Sample Iris Image.”

[9] John G. Daugman, “Anatomy, Physiology, and Development of the Iris,” <http://www.cl.cam.ac.uk/users/jgd1000/anatomy.html> (12 April 2006).

[10] Daugman, “Anatomy, Physiology, and Development of the Iris.”

[11] Daugman, “Anatomy, Physiology, and Development of the Iris.”

[12] International Biometric Group, “Iris-Scan: How It Works,” <www.biometricgroup.com/reports/public/reports/iris-scan_tech.html> (12 April 2006).

[13] Daugman, “Anatomy, Physiology, and Development of the Iris.”

[14] Iridian Technologies, “Iridian Technologies: Products,” <http://www.iriscan.com/products.php> (14 April 2006).

[15] EyeTicket Corporation, “EyePass,” <http://www.eyeticket.com> (5 May 2006).

[16] EyeTicket Corporation, “EyePass.”

[17] EyeTicket Corporation, “EyePass.”

[18] Iridian Technologies, “Iridian Technologies: Products.”

[19] Iridian Technologies, “Iridian Technologies: Products.”

[20] Iridian Technologies, “Iridian Technologies: Products.”

[21] Iridian Technologies, “PrivateID and KnoWho Authentication Server Product Description,” <http://www.iriscan.com/products.php> (15 April 2006).

[22] Iridian Technologies, “PrivateID and KnoWho Authentication Server Product Description.”

[23] Iridian Technologies, “PrivateID and KnoWho Authentication Server Product Description.”

[24] Iridian Technologies, “PrivateID and KnoWho Authentication Server Product Description.”

[25] Iridian Technologies, “PrivateID for Windows API,” January 26, 2002.

[26] Ian Sommerville, *Software Engineering*, 6th edition (Reading, MA: Addison-Wesley, 2001).

[27] Sommerville, *Software Engineering*.

[28] Douglas Bell, *Software Engineering: A Programming Approach*, 3rd edition (Addison-Wesley, 2000).

HUSSEIN FAKHRY, PhD, PEng is an Assistant Professor at Dubai University College, U.A.E. He received a PhD degree in Computer Control Systems and Robotics from University of Waterloo, Canada. Dr. Fakhry's research interests are mainly related to information systems, software engineering, computer control systems, robotics and applications of artificial intelligence. His current research interests include software systems architectures, modeling and simulation, IRIS recognition, and information systems security. He has worked for industry on many projects in control systems and SCADA systems. He is a member of a number of professional associations and networks including IEEE and IASTED.

BERNARD B. CARDOZO is a Senior Systems and Database Administrator at Dubai Naturalization and Residency Department (DNRD). He holds a Masters Degree (MSc.) in Computing and Information Systems from University of Hull, UK. Mr. Cardozo has more than 13 years of experience in the IT Industry. He has experience in the areas of project management, system analysis and design, programming, systems integration, database administration, distributed database architectures and data replication. He has been involved and has worked on major projects in DNRD such as Electronic Gate (EGATE) at Dubai Airport, Iris Recognition, Ports System and other major application modules.