Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 8th, 2009

Face Biometric Systems

Jackie Abbazio, Sasha Perez, Denise Silva, Robert Tesoriero, Frederic Penna, and Robert Zack
Seidenberg School of CSIS, Pace University, White Plains, NY, 10606, USA
{ja35743p, sp23747n, ds53227n, rt62098p}@pace.edu, fredpenna@verizon.net, robert.zack@stpart.com

Abstract

The objective of this study is to research and test various types of face recognition software to identify an individual's photo from a photo database. Face Biometric Systems utilizes software to compare an individual's photos against a database of photos as a way to identify and/or authorize individuals. Algorithms measure key points of the face (nose, eyes, mouth, jaw, etc), head angle, skin tone, lighting, and create a template based on these measurements. The file is then compared to other files (still photos or video captures) that are enrolled into the software's database, searching for a match based on the "Similarity Rating" percentage. The closer the characteristics match, the higher the similarity rating. The software can also identify individuals over time for various facial expressions.

1. Introduction

In today's world there is a growing concern regarding identity theft, national security, and on-line terrorism (DoS, viruses, worm, Trojan horses). There needs to be a way of protecting an individual's identity, businesses' websites, or government interests from attacks through on-line or electronic intruders. There needs to be steps in place that can help in determining that a person is who they claim to be and not someone impersonating them. It is at this point where the science of biometrics comes into play. Biometric science utilizes the measurements of a person's behavioral characteristics (keyboard strokes, mouse movement) or biological characteristics (fingerprint, iris, nose, eyes, jaw, voice pattern, etc). It is these measurements that are then used to create a reference template, which the recognition software uses to identify or authorize an individual as the person they claim to be.

Biometric identification is any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identify of an individual [3]. The study uses face biometric software to provide face recognition through computer analysis of facial structures based on facial characteristics. These characteristics are measurements consisting of inner and outer eye length, nose, mouth, feature angles, length of various portions, and facial positions. Pattern recognition software relies on "Data Collection" (raw image data), "Feature Extraction" (eyes, nose, mouth, etc), and "Classification" (male/female, skin tone) to create a template based on the mathematical algorithm (Neural-Networks, Eigenface) of the measurements to build and store a file within the software database (enrolled images). It is this database that will be used for the comparison between a subject's image and the database for identification purposes. Several face recognition software were researched and tested. The main focus was to see whether a 2-dimensional photo database is capable of distinguishing age recognition of an individual, identify the similarities of an individual from others in a group, or be used in a way of providing security for PDA devices.

Relevant research into the field of face biometric science has focused more on the advancements of the science, changing the direction of face recognition from 2D image recognition to 3D image technologies. For example, research in 3D face recognition focuses on the use of 3D scanners to capture the data and provide accurate 3D face recognition [11].

2. Research Methodology

Several face recognition software available in the market today were evaluated against the requirements listed in Table 1. It was important that the software met the following criteria's: below price threshold of $400, able to accept different lighting, accept various head rotations, and accessible demo version for testing. Luxand FaceSDK 1.7 and VeriLook 3.2 were chosen to analyze face biometrics because they both had demo versions with GUI interface and complied with most of the requirements. Authentication and age recognition tests were run on both Luxand FaceSDK and VeriLook 3.2. Each test had different sizes of sample test photos, at various poses, photo

quality/resolution, and was tested at different false acceptance rate (FAR). For the age recognition tests, the data set included photos of individuals from infancy to adulthood. The identification tests included a second set of images containing 29 photo mug shots of the students in the Capstone Project course. All test cases were performed on demo versions of the software.

Item	FaceSDK1.7 *	ActiveX DLL 1.1	Fast Access	VeriLook 3.2*
Cost	$450.00	$399	$329	€ 339.00
Captures Video	No	Yes	No	Yes
Works with	Cameras/ webcam	Webcam	Cameras/ webcam	Cameras/ webcam
Accepted Resolution	Low-High	Low-High	Low-High	High
Accepted Poses	Head rotation up to 30° degrees from frontal (nodded, rotated, or tilted)	No info provided	Full frontal	Head rotation up to 10° degrees from frontal (nodded, rotated, or tilted)
Accepted Lighting	Good	No info provided	Various	Good
Source Code Available	No	Yes	No	Yes in special licensing agreement only
Platforms	Windows	Windows	Windows	Windows, Linux, Mac

*Free Trial Version
Table 1: Software Comparison Table

2.1. Luxand FaceSDK 1.7

Luxand FaceSDK 1.7 is a face detection and recognition library that is integrated into the user's application and offers the Application Programming Interface (API) the ability to detect similarities in facial characteristics [4]. FaceSDK contains a face identification algorithm that automatically searches a face within a database and identifies the user based on a facial photograph. Upon facial detection, FaceSDK will plot and process facial coordinates based on eyes, eye corners, eye brows, mouth, nose, nose tip, etc. Comprehensive FERET tests were performed to confirm the reliability of the Luxand FaceSDK technology. FERET is a testing protocol that was designed in September 1996. This database allows algorithm performance to be computed for identification and verification evaluation protocols for a variety of different *galleries* and *probe* sets. According to the NISTIR 6281 technical report, a *gallery* is a set of known individuals and a *probe* is an unknown face presented to an algorithm [6].

FaceSDK face detection specifications are as follow: Frontal face detection with the ability to detect multiple faces in a photo, supported head rotation of -30 to 30 degrees of both in-plane and out-of-plane rotation, detections speed from 0.05 to 1.1 seconds, returned information of detected face based on (x, y) coordinates of face center, width and rotational angle. Configuration of face detection parameters is easy with a library size of 1.6 megabytes. Facial feature extraction detection is based on 40 facial feature points (eyes, nose, mouth, etc). FaceSDK has the ability to match two faces within the given FAR and FRR, contains an enrollment time of 0.3 seconds (this does not include face and facial feature detection), includes template size of 5.4 kb and matching speed of up to 5,000 faces per second.

2.1.1. System Requirements

Luxand FaceSDK is supplied as a Win32 Dynamic Link Library (DLL) that can be used with a number of Win32 platforms. Contains interface header files along with sample applications that work with Microsoft Visual C++ 6.0/7.0/2005/2008, Microsoft .NET, and Borland Delphi 6.0/7.0. FaceSDK runs on the following Windows platforms: Windows 98, ME, 2000, NT or XP. 128 MB of RAM and 100 MB of free space are needed on the application to install and run FaceSDK.

2.1.2. Software Installation

The demo software was downloaded from the Luxand website [4]. From the Luxand website click download and perform the following actions: Download Luxand FaceSDK version 1.7, Run/Save Luxand_FaceSDK_setup.exe, (Setup dialog box) click on Run, If the Internet Explorer Security Warning dialog box appears click "Run", (License Agreement) click "Accept" radio button & then click "Next", (Destination Folder) click on "Next", Click on "Install", Click on "Finish". Luxand FaceSDK 1.7 is now installed on your computer in the "Programs" menu.

2.1.3. Test Procedures

The procedures followed to test Luxand FaceSDK 1.7 are as follow:
Create a folder in your computer with the images you want to enroll and images that will be used for testing facial recognition.
Open Luxand FaceSDK that is in your Programs File
Click on Tool > Option
Change Minimal Face Quality to 1 and FAR to 100 and click OK
To enroll images click on Files > Enroll Face(s)
Browse your database folder
Select all images you want to enroll and click Open.

Luxand FaceSDK will enroll the selected images. To match an image against the database:
Click on File > Match Face
Browser to folder of images you want to match
Select the image you want to test and click Open
FaceSDK will open a results Window like Figure 3.

2.2. Face Recognition ActiveX DLL 1.1

Face Recognition ActiveX DLL software allows a user to create their own biometric face identification security for Windows. The software uses a neural network back propagation algorithm combined with more Artificial Intelligence tool added for imaging optimization [9]. Back propagation networks learn by example; therefore, the neural network back propagation provides a learning set that consist of some input examples and known-correct output for each neural case. The software will use the input-output examples to show the network the expected behavior and the back propagation algorithm will then allow the network to adapt [5].

The demo version for Face Recognition ActiveX DLL supplied the image database, which, consisted of small black and white images. The software did not contain options to change the settings such as FAR, FRR or MFQ. Due to limitations of the demo; test experiments could not be executed and no data is available.

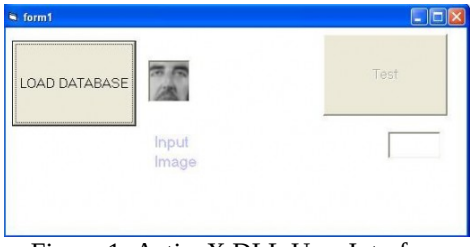

Figure 1: ActiveX DLL User Interface

Figure 2: ActiveX DLL Sample Image Database

2.3.

2.4. Sensible Vision FastAccess

Sensible Vision has created a face recognition system designed for security authentication for personal computers. FastAccess provides computer access control without the end user ever lifting a finger. No password is required instead a user accessing their workstation will automatically be logged on via face authentication. As soon as the user leaves the workstation, they are automatically logged off. The capabilities extend to other authorized users as well. For example, if an authorized user sits in front of a computer that is not their own, the system will authenticate and log the user on. The main purpose of the software is to secure access to windows operating systems.

Sensible Vision has a unique patent pending learning algorithm, called the Continuous Sensing Adaptive (CAS) technology. According to the Sensible Visions website, CAS technology creates each numerical template by measuring 150-1000 features on a user's face. Particular emphasis is placed on the eyes and nose, providing greater tolerance to changes in hair style, head position and facial expression. With so many points of comparison, CAS has the detail to minimize the likelihood of incorrect recognition [10].

Sensible Vision sells the evaluation kit for $329 with the underlying goal for their customers to purchase the Enterprise Package. The Enterprise Package is available to purchase with a minimum of 100 workstations. The Software kit includes: 3 Permanent Licenses, 3 Cameras and Evaluation kit only. Demo versions are not available for download on the company's website, for this reason test experiments could not be executed and no further data is available.

2.5. Neurotechnology VeriLook 3.2

VeriLook 3.2 is face recognition software that is designed for biometric system developers and integrators. It allows easy integration and rapid development of biometric applications using functionality from the VeriLook algorithm [8]. VeriLook can perform simultaneous multiple face detections with the ability to process 100,000 faces per second and it recommends the minimum image size to be 640x480 pixels [7].

The algorithm has been tested with standard face databases, such as FERET and XM2VTSDB. As explained earlier in section 2.1, FERET is a database containing gallery and probe sets to compute identification and facial evaluation protocols.

XM2VTSDB is a large multi-modal database, which enables researchers to test multi-modal face verification algorithms. The database includes recorded speech and tilted head movements from 295 volunteers from the University of Surrey [1].

The demo version for VeriLook had a poor enrollment rate of 15%. Four high resolution images from the data set were enrolled and tested at an FAR set to 1%, 25%, 50% and 100%. Due to a very low enrollment rate, this software could not be used for the classmates similarity match experiment performed on Luxand FaceSDK.

2.5.1. System Requirements

PC or Mac with a 2GHz processor (or better), UDP and TDP network support, MySQL or Oracle server, Windows 2000/XP/2003/Vista, Linux 2.6, GCC-4.0, pkg-config-0.21, GNU Make 3.81 (or newer versions of either). Additional requirement for VeriLook Matcher and Extractor are: Microsoft DirectX 8.1, Linux Video4linux, Mac OS x, QuickTime 6 (or newer).

2.5.2. Software Installation

From the Neurotechnology website [8], download the "Vlook.zip" file and save the file to a folder of your choice (or run directly from the dialog box). Extract VeriLook files, select VeriLook file and run software installation. VeriLook is now installed. A short cut can be placed on the desktop for quicker running of the program.

2.5.3. Test Procedures

Create a folder in your computer with the images you want to enroll and images that will be used for test.
Open VeriLook 3.2
Click on Tool > Options
Change Face Quality Threshold to 75 to 1 and FAR to 100 and click OK
To enroll images click on Jobs > Enroll
Browse your database folder
Select all images you want to enroll and click Open.

VeriLook will enroll the selected images. To match an image against the database:
Click on Jobs > Match
Browser to folder of images you want to match
Select the image you want to test and click Open
VeriLook will match the selected image against the database and display results

3. Results

As mentioned earlier, the goals of this study were to test and recommend face recognition software that is: 1) able to identify and authenticate, 2) serve as a platform for PDA security, and 3) identify people's aging. The specific experiments performed and results are described below. The first and second experiment included the headshot of 29 classmates to test similarity matches. The same database was also used to train the software. A third experiment included a database of aged photographs from team members to test age recognition.

3.1. Luxand FaceSDK 1.7 Results

Luxand FaceSDK 1.7 uses face biometric feature extraction to match subject's faces against the enrolled database. FaceSDK's threshold was lowered by setting the FAR (False Acceptance Rate) to 100%. The FAR is the probability that the software will incorrectly declare a successful match between the input data against the database [2]. In a security setting, FAR should be set to less than 1% to avoid authenticating individuals inaccurately. The minimum face quality (MFQ), which, is the threshold the software will recognize a face in an image, was set to the lowest quality of 1 to ensure that all of the images were enrolled successfully.

FaceSDK enrolled all 29 images from students in the Capstone Project course at an average rate of 0.9 seconds per photo. The system was tested with a False Acceptance Rate (FAR) set to 1%, 25%, 50% for age recognition and 100% for similarity match testing. Every image matched 100% against the exact image in the database. We concluded that the FaceSDK software has a minimum similarity threshold of 47%. Although, this is not stated in any Luxand documentation, after extensive testing the software did not produce a similarity match below 47%. For this reason, the maximum number of matches received was 26 out of 29 images in the database. Figure 3 displays a partial screen of the headshot containing the highest number of similarity matches.

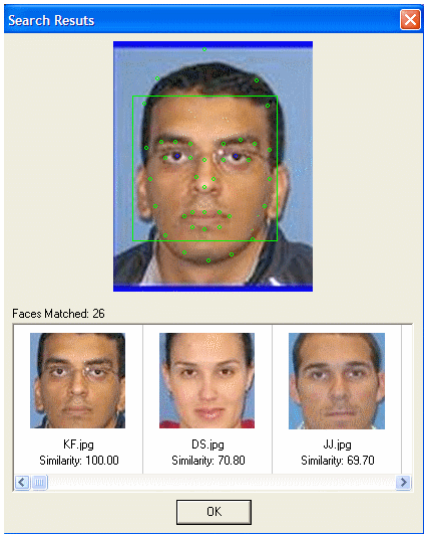

Figure 3: Face with Highest Similarity Matches

Conversely, other subjects on our database only received a few matches with the lowest being four matches. The complete similarity matrix with the results of this study can be found in Appendix A. Figure 4 shows the output of Luxand FaceSDK for the first five images in alpha order on our database and their closest similarity match. The image in the first column of Figure 4 is the image matched against the database. The next two images are the two closest matches and their similarity percentage.

Figure 4: Luxand FaceSDK output for the first five images on the database

FaceSDK worked relatively well with identifying facial aging. Again, the FAR was set at 100% and the minimum face quality was set to 1. For this test, the data was divided into training and testing sets. In Figure 5, the software correctly identified an image from 1969 with an image of the same subject taken in 2008 with 61.9% similarity rate. The next highest matches were pictures from 2007 and 1996 with similarity rate of 60.6% and 59.2% respectively. Although the software identified the subject correctly, it did not match the subject in chronological order. If the software were truly measuring age, the results should have been in chronological order.

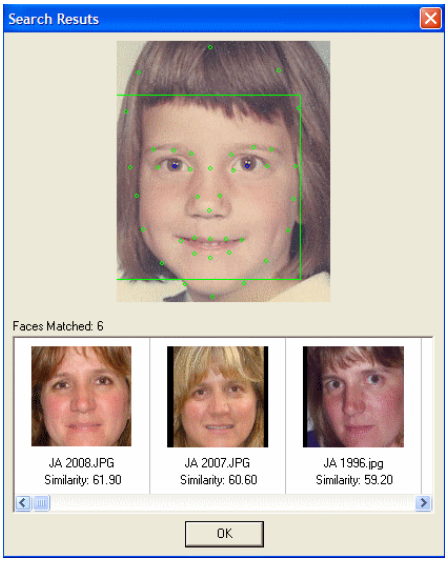

Figure 5: Aging Identification Test

3.2. VeriLook 3.2 Results

VeriLook 3.2 demo allows users to enroll an image into the software, processes the face, extracts the features, and creates a template within the database. The matching mode will perform an image match against face templates stored in the database. Facial characteristics, expressions, and image resolution all have an effect on the software results. Two experiments were performed to test this software for identification and age recognition.

The demo version had a low enrollment rate because it only accepted high-resolution photos. Therefore, our two experiments only included a database of four high-resolution photos from the team members. The face quality threshold controls how strict rules are applied when determining the quality of a face for

extraction. For the experiment the face quality was lowered to 75 to ensure all photos were enrolled successfully.

For the authentication experiment the False Acceptance Rate (FAR) was set to 100%. The four photos in the database were matched against the same four photos (Figure 6). All images matched 100% against the same image in the database. The score of 180 is interpreted as an exact match. In order to compare the VeriLook software to the FaceSDK software, the data was normalized by converting the 180 score to 100%. The other scores were than converted to a percentage. After extensive research into the VeriLook software no documentation was found to explain the similarity score of 180. The exact experiment was performed on the FaceSDK software to accurately compare the similarity matches against VeriLook. The data results are shown in Table 2 and 3. FaceSDK similarity and facial detections were notably higher than VeriLook. Excluding exact matches, FaceSDK had a high similarity rate of 58.3% versus VeriLook's high of 11.0%. Figure 7 depicts the output of the similarity match of image SPer.jpg against the four enrolled images in the database.

Figure 6: Images enrolled on Luxand and VeriLook comparsion test

VeriLook 3.2 Similarity Matches				
	DS	JA	RT	SPer
DS	100			4
JA		100		
RT			100	11
SPer	4		11	100

Table 2: VeriLook Identification and Authentication Results

FaceSDK 1.7 Similarity Matches				
	DS	JA	RT	SPer
DS	100	58.3		
JA	58.3	100	53.1	52.4
RT		53.1	100	52.7
SPer		52.4	52.7	100

Table 3: FaceSDK Identification and Authentication Results

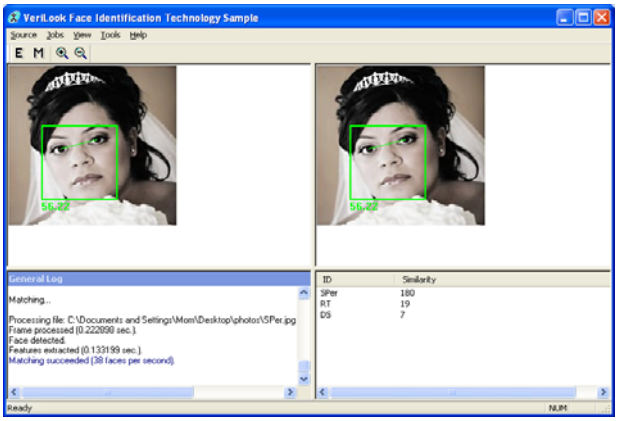

Figure 7: VeriLook Match Output

For the identifying age experiment the FAR was set to 100%. The four photos in the database were matched against photos of the same persons from past years. Photos had to be of a high resolution to enroll successfully into VeriLook. The results yielded only two matches. One example of the results is below (Figure 8). The results show that the photo from 1969 matched a photo from 2008 with a similarity score of 18 or 10%. This result is comparable with the FaceSDK age identification test (Figure 5). However, the same image from 1969 matched the same photo from 2008 with a 61.9% similarity rate.

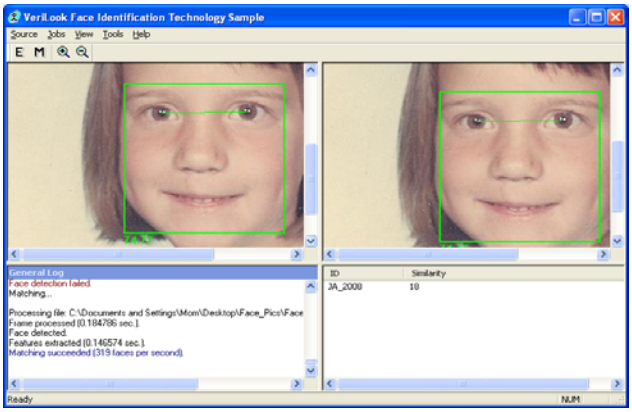

Figure 8: Age Identification Test

3.3. Results for a PDA Security Platform

As a tool to enhance personal digital assistants and mobile computing device (PDA) security, facial biometric software was evaluated and used to perform experiments. Some of the experiments evaluated the capabilities of the selected software to determine the viability of the technology for use in PDA User Authentication applications. As a result of this work, a required minimum acceptability standard for security applications was not met and the selected product is

not suitable for use in the role of a PDA User Authentication. The results of the experiments indicate that while it may be useful as part of a multimodal solution that incorporates other technologies, facial biometrics using the selected software is not sufficient on its own to meet the minimum acceptability standard. The results of the preliminary experiments indicate that the software produced inconsistent results in comparing the subjects under study against the enrolled database of subjects. Although the feature extraction algorithm appeared to work well, the inability of the software to accurately identify the unique characteristics of the same subject from the enrollment database when evaluating subject photographs makes it unsuitable for use in a security context.

A person's face appears to have the desirable characteristics of universality and uniqueness that are important parameters in a biometric security system. For the subjects under study, the software performed well and has the potential to integrate into security applications that are easy to use and convenient for the user. Unfortunately, the test results did not yield acceptable and consistent results, which are a core requirement in any security solution. In addition, it appears that the software can easily be circumvented due to its inability to consistently and accurately match subject features against the enrollment database. From the results produced, the False Acceptance Rate needed to be set to a high percentage to even return matches. These material observations disqualify the selected software as a security application. Further work is needed to determine if other solutions that utilize facial biometrics will yield better results.

Since the obstacles of variable lighting and shadows appear to have contributed to the test results, further work in the areas of 3-D facial biometrics that use near infrared and infrared light to see beneath the skin and are not sensitive to shadows and variable lighting conditions offer promise for using the face as a biometric in securing PDA's on its own or in combination with other security measures.

4. Conclusion and Further Work

Face biometric techniques can be used for both authentication and identification applications. These applications have a critical role in national and economic security. At present many are focused on three-dimensional techniques. This study researched several face recognition software and tested Luxand FaceSDK 1.7 and Neurotechnology VeriLook 3.2. The objective was to find and recommend software capable of indentifying face similarities of an individual from others in a group, distinguishing age recognition and providing security for PDA devices.

Luxand FaceSDK 1.7 works very well in identifying face similarity among people in a group. FaceSDK also worked relatively well matching an image of the subject as a child with a recent image of the same subject with 61.9% similarity rate, thus recognizing aging. FaceSDK was the preferred software from both user-friendliness and performance in terms of matching face similarity and recognizing aging.

VeriLook 3.2 had more limitations than FaceSDK. It only accepted high-resolution images, which limited ours tests to four high-resolution images. VeriLook results for the similarity test were lower than the FaceSDK software. Although there were no claims on VeriLook's documentation claiming it recognizes images, VeriLook did match an image from 1969 with an image from 2008 of the same subject with a 10% similarity score.

None of the software tested was suitable for PDA security use. Test results did not yield acceptable and consistent results, which are a core requirement in any security solution. Variable lighting and shadows appear to have contributed to the test results. Therefore, we recommend further work using 3-D face biometrics software and scanners to find optimal solution for PDA security.

5. References

[1] Chan, Chi Ho, *The Extended M2VTS Database*, http://www.ee.surrey.ac.uk/CVSSP/xm2vtsdb/ (17 November 2008).

[2] Czyz, J., Havran, C., Hupet, L., Lee, J., Vandendorpe, L., Verleysen, M. (2002), *Independent Component Analysis for face authentication*, www.dice.ucl.ac.be/~verleyse/papers/kes2002ch.pdf > (03 November 2008).

[3] Gartune, J and Thomas, A, Woodward, J, Horn, C, (2003), *Biometrix a Look at Facial Recognition*, www.rand.org/pubs/documented_briefings/DB396/DB396.pdf (04 November 2008).

[4] Luxand Inc, http://www.Luxand.com, Copyright 2005-2008, (2 November 2008).

[5] McCollum, Pete (1998), *An Introduction to Back-Propagation Neural Networks*, http://www.seattlerobotics.org/encoder/nov98/neural.html (17 November 2008).

[6] Moon, Hyeonjonn, Phillips, Jonathan P., Rizvi, Syed A. (1998) *The Feret Verification Testing Protocol for Face Recognition Algorithms*, http://www.itl.nist.gov/iad/humanid/feret/doc/feret_verification_nist_ir_6281.pdf (17 November 2008).

[7] Neurotechnology, www.neurotechnology.com, (10 November 2008).
[8] Neurotechnology, http://neurotechnology.com/verilook.html (17 November 2008).
[9] New Free Downloads, http://www.newfreedownloads.com/Software-Developer/Active-X/Face-Recognition-ActiveX-DLL.html (17 November 2008).
[10] Sensible Vision, http://sensiblevision.com/technology/cas.htm (17 November 2008).
[11] Sun, Yi, Yin, Lijun of the, *Genetic Algorithm Based Feature Selection Approach for 3D Face Recognition*, State University of NY at Binghamton, http://www.biometrics.org/bc2005/Presentations/Conference/1%20Monday%20September%2019/Poster%20Session/final_biomeSymp_Yin_Lijun.pdf (01 November 2008).

APPENDIX A

Classmates Face Similarity

	AB	AG	AN	CF	DB	DL	DS	EU	FH	FM	JA	JF	JJ	KF	KJ	MC	MS	MT	NWh	NWw	QB	RE	RO	RT	RW	SPer	SPet	SV	YK
AB	100.0			53.5	53.9		60.7	53.1		51.4	53.3	56.0	55.5	61.1	63.4	61.8	54.6		50.0	62.7		57.5	56.9			56.1	52.2	61.1	
AG		100.0					52.9				49.9					48.8				48.7			48.4							
AN			100.0				34.8									30.6	47.7									47.6		48.0	
CF	53.5			100.0	54.4		54.1	56.1		57.6	52.7	54.5	64.8	66.6	58.6	59.3	53.5	47.3	66.8	56.4		54.8	56.7	57.3		63.2	53.0	51.0	
DB	53.9			54.4	100.0	55.0	55.2	52.9		54.8	53.1	58.7	55.2	58.3	62.6	60.2	58.9		53.6	62.4		55.7	62.3		47.0	51.2	48.8	54.6	
DL					55.0	100.0	63.0			48.2		55.4	66.0	65.1	57.3	49.0	48.5		48.4	50.4	47.6	55.0	58.0					57.1	
DS	60.7	52.9	54.8	54.1	55.2	63.0	100.0	52.0		51.2	53.0	56.0	71.3	70.8	60.2	60.6	58.3		60.0	56.0	48.2	56.0	61.3		47.8	55.1	56.5	63.9	
EU	53.1			56.1	52.9		52.9	100.0		54.7	48.2	52.3	57.1	49.0	49.6	55.3	53.0		54.9	51.0		55.0	50.6			59.0		53.8	
FH									100.0	49.0		58.4	49.1	50.4	47.0		54.4		54.7			60.7						50.5	
FM	51.4			57.9	54.8	48.2	51.2	54.7	49.0	100.0	53.2	62.6	56.2	51.1	56.3	50.6	53.7		49.3			59.7	48.4	48.5		55.5		60.7	
JA	53.3	49.9		52.7	53.1		53.0	48.2		55.2	100.0	58.6	57.3	53.8	59.5	55.3	57.6		56.5	52.8		56.5	47.9	53.1		52.7		59.1	
JF	56.0			54.5	58.7	55.4	56.0	52.3	58.4	62.6	58.6	100.0	68.4	62.6	61.8	58.0	61.1	47.7	62.7	66.8	49.5	64.4	58.0	48.8		60.0	46.5	60.6	
JJ	55.5			64.8	59.2	66.0	71.3	57.1	49.1	56.2	57.3	68.4	100.0	69.7	65.1	57.2	63.4	53.7	65.3	66.0	47.7	63.3	58.2			58.2	57.0	70.1	
KF	61.1			66.6	58.3	65.1	70.8	49.0	50.4	51.1	53.8	62.6	66.7	100.0	67.0	59.3	58.7	49.7	62.1	64.0	50.2	59.4	59.9	48.6	49.7	53.3	52.5	63.3	
KJ	63.4			58.6	62.6	57.3	60.2	49.6	47.0	50.3	59.5	63.8	65.1	67.0	100.0	54.6	59.9	53.4	65.6	66.2	52.6	60.7	63.7	52.3		60.9	58.7	60.7	48.4
MC	61.8	48.8	30.6	59.3	60.2	49.0	60.6	56.3		50.6	55.3	58.0	57.2	59.3	54.6	100.0	57.6		57.9	60.8		58.9	50.4	55.7		58.5	48.3	63.0	
MS	54.6		47.7	53.9	58.9	46.3	58.3	53.0	54.4	53.7	57.6	61.1	65.4	58.7	59.9	57.6	100.0		61.9	49.7		62.0	57.4	49.4		54.2	53.0	57.6	
MT				47.3								47.7	55.7	49.7	53.4			100.0	54.1										
MWh	50.0			66.8	53.6	48.4	60.9	54.9	54.7	49.3	56.5	62.7	66.3	62.1	63.6	57.5	61.5	54.1	100.0	54.8	49.2	58.7	52.0	51.9		59.6		57.7	48.0
MWw	62.7	48.7		56.4	62.4	50.4	59.9	51.0			52.0	66.8	66.8	64.0	60.2	60.8	59.7		54.8	100.0		56.1	58.6	50.0		58.1	54.9	55.7	
QB						47.6	48.2					49.5	47.7	50.2	52.6				49.2		100.0	48.3	49.9					53.2	
RE	57.5			54.8	55.7	56.9	56.0	55.0	50.7	59.7	58.5	64.4	63.3	59.4	60.7	56.9	62.0		58.7	56.1	48.3	100.0	48.9	48.8		53.6		59.6	47.4
RO	56.9	48.8		56.7	62.3	50.0	61.3	50.6		48.4	47.9	58.0	66.2	59.9	63.7	50.4	57.4		52.0	66.8	49.9	48.9	100.0	50.4			56.8	51.9	
RT				57.3						48.5	53.1	48.8		48.9	52.3	55.7	49.4		51.9	50.0		48.8	50.4	100.0	47.1	55.2			
RW					47.0		47.9							49.7										47.1	100.0	48.6			
SPer	56.1		47.8	63.2	51.2		55.1	50.0		55.5	52.7	58.0	58.2	53.3	60.9	58.5	54.2		58.8	56.1		53.6		55.2	48.6	100.0		60.1	
SPet	52.2			53.0	48.8		56.5					49.5	57.8	52.5	50.7	49.3	53.9			54.9			56.6				100.0		
SV	61.1		48.0	51.0	54.8	57.1	63.9	53.8	50.5	60.7	59.1	60.6	70.1	63.3	60.7	63.0	57.6		57.7	55.7	53.2	58.8	51.9			60.1		100.0	
YK															48.4				48.0			47.4							100.0

Appendix A: Face Similarity Matrix using Luxand FaceSDK 1.7 software.