TACIDS: Tactical Identification System Using Facial Recognition

Award # 2007-RG-CX-K001

Submitted by:
The Automated Regional Justice Information System

Submitted to:
U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Tactical Identification System

TABLE OF CONTENTS

CONTENTS

ABSTRACT 4
BACKGROUND 5

STATEMENT OF THE PROBLEM 5

PURPOSE 6
RESEARCH AND DESIGN METHODS 7
LOCAL OUTREACH 8
TACIDS MARKET RESEARCH PROCESS: 10
SITE VISITS AND PRODUCT DEMOS 14
RESEARCH FINDINGS: 14
IMPLICATIONS FOR POLICY AND PRACTICE 17
MOBILE APPLICATION TECHNICAL APPROACH 17
DATA SOURCES 18
MOBILE DEVICE SELECTION 19

..... 21

SECURITY REQUIREMENTS 21

FUNCTIONAL GOALS AND REQUIREMENTS 23
ACCESS CONTROL & AUDITING 28
ERROR HANDLING 29

TACIDS OUTCOMES 29

NEXT STEPS 34
CONCLUSION 36

TACIDS: Tactical Identification System Using Facial Recognition

ABSTRACT

ARJIS, the Automated Regional Justice Information System, a consortium of 82 local, state, and federal law enforcement agencies was awarded a grant to develop a mobile tactical identification and query system based on facial recognition for use by law enforcement officers and investigators. To initiate this effort, ARJIS completed extensive research on current technologies and standards to include a market survey and evaluation of facial recognition products. One of the top-rated facial recognition algorithms was then identified, along with state of the art biometric processing technology as the basis for building the mobile application.

ARJIS added an encoding process and a web services component in its existing suite of law enforcement tools which allows an officer in the field to take a photo, select one of several available image repositories and upload it to a server-side component which matches it against the over 1,300,000 booking photos in the San Diego County Cal-Photo mugshot node and the more than 93,000 images contained in the Chula Vista Police Department's Offender Track booking system. Positive matches are then processed on the server side and a gallery of potential candidates is sent back to the law enforcement agent for comparison.

If the agent identifies a positive match from the photo lineup, a query may then be initiated against ARJIS ONASAS (Officer Notification and Smart Alerting System), County Warrants, NCIC, DMV and CLETS, Nlets and ARJIS regional incidents via the SRFERS application. All data returned from the query along with the positive match is then sent back out to the agent in the field. Also built into the application is the ability for officers to search existing TACIDS records, and to create and upload electronic field interview incident records to accompany images captured in the field.

This solution allows agents in the field to positively identify and query for relevant data on individuals who have been stopped or arrested, but can't be immediately identified based on information given by the subject. Ultimately it leverages the existing base of more than 500 ARJIS wireless device users in the San Diego region, each equipped with a digital camera and broadband connection, and the San Diego booking photos housed and maintained by ARJIS.

The ARJIS Wireless Program has shown great success at providing information to law enforcement entities working in the field quickly, securely and reliably, and this project gives them another tool to expand their capabilities. Furthermore, it saves officers time by eliminating the need to transport persons to a police facility and enhances officer safety by reducing physical contact officers often have to make when individuals are not being cooperative.

BACKGROUND

Many investigators and patrol officers spend the majority of their shift away from the office and outside of their vehicles. Often time this results in delays getting suspect and vehicle responses over the radio from dispatchers who have higher priorities. Too often potential suspects are misidentified, or released before positive identification can be confirmed.

Wireless technology has progressed to the point where it is being embraced by law enforcement more than ever before. This has set the stage for enhancing the ability for officers to gain access to mission critical information that was never before possible. With that said, positive identification of individuals detained and suspected of criminal activity is still a challenge. In many cases, photo images are accessible through wireless devices but that assumes that the officer has a name, or other biographical data to search on. Facial recognition technology uses the biometric characteristics of the face itself in order to search on similar images within a database, providing yet another mechanism of identifying these people.

Combining the facial recognition technology with that of a wireless device that's already equipped with a built-in digital camera provides a unique opportunity to build a law enforcement application that is capable of not only assisting in the positive identification of a person, but can be further leveraged into the creation of new field interview or suspicious activity records, complete with new digital images and automated date, time and geographic stamps. These records then become part of the data pool for future queries.

In an effort to pilot an implementation of mobile facial recognition technology for peace officers, in 2007 NIJ awarded a grant to the Automated Regional Justice Information System (ARJIS) to develop an information sharing proof-of-concept, known as TACIDS (Tactical Identification System).

STATEMENT OF THE PROBLEM

Often as law enforcement entities work in a tactical environment they encounter individuals unwilling to cooperate and give accurate information. Sometimes, this lack of cooperation renders it impossible to positively identify the individual. With limited

cause officers may be unable to detain these persons long enough to confirm their identity and thus miss an opportunity to detain a wanted person.

Peace officers have multiple tools at their disposal to assist in the identification of persons that are contacted, starting with photo identification carried and displayed on demand. In many contacts, officers have had prior contact and are already familiar with the person's identity. Other traditional methods include asking pertinent questions and then verifying through Department of Motor Vehicle driver's license and registration records and in the case of ARJIS, verifying against incident records. More recently, field personnel have had access to mug shot photos and California driver's license photos, where they can make a visual comparison between those photos and the persons standing in front of them.

While these tools have been a tremendous help, there is nothing to assist when the person of interest gives totally false and unverifiable information. When all else fails and if probable cause for an arrest exists, the person can be handcuffed and transported to a facility where fingerprints can provide positive identification. This process is timely and can put officers at risk, as uncooperative individuals can turn violent.

PURPOSE

Real-time, automatic access to facial recognition tools can be extremely valuable in situations where ascertaining an individual's identity is an essential element of a crime. Most importantly, knowing the identity of a suspect allows officers to more accurately evaluate and predict potential dangers that may arise during an investigative stop.

ARJIS and its member agencies have had tremendous success with its mobile wireless program. ARJIS law enforcement users can utilize their laptops, tablets or smart phones through a secure, private, wireless network to access information which can help positively identify wanted individuals. The program currently supports more than 500 users and has helped detain numerous people who would have otherwise been released based on lack of probable cause. A facial recognition platform used on a case-by-case query will add to the existing tools which law enforcement agents use in the positive identification process.

The overall budget for the TACIDS project was $418,000. This project was supported by a grant awarded by the National Institute of Justice (NIJ), number 2007-RG-CX-K001, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice. NIJ defines publications as any planned, written, visual or sound material substantively based on the project, formally prepared by the grant recipient for dissemination to the public.

RESEARCH AND DESIGN METHODS

Facial recognition is a relatively new concept that ARJIS had little experience with prior to this grant. In order to gain an understanding of current biometric standards, facial recognition products, algorithms and how the technology can best benefit law enforcement, ARJIS completed extensive research on each of these topics. This research included a market analysis of products and algorithms, meetings and demonstrations with vendors, internet research, participating on biometric committees, and conducting focus groups with law enforcement officers.

Participation in Biometric Committees and Focus Groups:

It is the policy of ARJIS to involve the law enforcement user community in the research, design, development and testing of new applications. ARJIS also strives to work directly with the member agencies as well as federal agencies at the national level in order to leverage existing resources and to work in concert with its partners.

FBI Biometric Center of Excellence (BCOE) and Cal-DOJ

The BCOE is the FBI's program for exploring and advancing the use of new and enhanced biometric technologies and capabilities for integration into operations. The information provided by the BCOE assisted ARJIS in understanding the history of facial recognition and the current status of the technology. After researching this program, ARJIS reached out to BCOE and was invited to Clarksburg, WVA for further discussion on standards and policies.

At this time, ARJIS was also working with CAL-DOJ to ensure the TACIDS project would be consistent with the states biometrics standards and policies. ARJIS participated in several CAL-DOJ initiatives including 'Vision 2015', which incorporates facial recognition technology. ARJIS was asked by CAL-DOJ to participate on the FBI's Facial Identification Scientific Working Group (FISWG) to address the classification and individualization of human beings through the photographic comparison of their visible physical attributes such as face, ear, skin texture, and hair.

The FISWG develops consensus standards, guidelines, and best practices for the discipline of facial recognition. These standards were used in the development of the TACIDS platform. The main objectives of the working group are:

- Coordinate interaction of members of the relevant community for facial recognition to maximize collective resources;
- Document the scientific basis for facial recognition;

- Standardize the practices for facial recognition to include standard operating procedures and training;
- Advance the scientific basis by promoting collaboration, gap identification, and prioritization of specific research, development, test and evaluation topics;
- Promote the products of the FISWG to members of the pertinent operational communities, including criminal justice, intelligence, and identify management;
- Maintain currency of the above and respond to emerging challenges, such as technology advancement and legal requirements.

Nlets

ARJIS was invited to participate in a special workshop which convened in Chicago on December 8, 2010. The workshop was sponsored by Nlets (National Law Enforcement Telecommunications System) for the purpose of developing a model Privacy Impact Assessment report, which in turn produced a set of Policy and Procedure documents directly related to the use of facial recognition technology as applied to driver's license and mug shot photo images for law enforcement. Subject Matter Experts from ARJIS, FBI, New Jersey State Police, Illinois State Police, North Carolina Department of Motor Vehicles, Pinellas County Florida Sheriff's Department, Delaware State Police, Oregon State Police, New York State Department of Motor Vehicles, Cumberland County Pennsylvania District Attorney and the Chicago High Intensity Drug Trafficking Area participated in this event and all provided valuable feedback.

The final Nlets Privacy Impact Assessment and Policy and Procedure documents were completed in June 2011 and published shortly thereafter. These documents serve as the foundation for the ARJIS TACIDS polices and procedures.

LOCAL OUTREACH

ARJIS staff attended meetings with several user groups and joined a Technical Advisory Group (TAG) with the San Diego Sheriff's Department Crime Lab's Cal-ID division. This group held regional status meetings regarding mobile identification efforts funded by the California RAN Board. Topics ranged from regional Automated Fingerprint Identification System (AFIS) upgrade (from NEC to Cogent), to mobile fingerprint identification (MobileID), to the Sheriff's "Take Me Home" project to facial recognition technology in general.

These meetings were beneficial in setting the stage for a more global solution to biometric identification techniques while leveraging existing funding and technical resources in a more cohesive overall plan to provide field officers with the most comprehensive tools available.

Officers from multiple agencies were selected to participate in the TACIDS test portion of this project after the software solution was in place. ARJIS held multiple wireless focus groups with officers at the local, state, and federal level to obtain their feedback for the development of the use case and functional specifications.

Internet research to identify existing studies on the topic of facial recognition:

Internet research was completed to obtain info on existing standards, technologies and to determine if open source technologies could be leveraged for the development of TACIDS. This research helped guide the technical solution for the grant and several of the key documents are described below.

NIST Facial Recognition Studies

NIST (National Institute of Standards and Technology) – The NIST website was consulted for any and all documentation relative to Facial Recognition standards. Pertinent documents were downloaded and reviewed. The most recent activity sponsored by NIST includes several reports that were published in 2011 and 2012. The ANSI/NIST-ITL Standard Update for 2011 (Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information); the Report on the Evaluation of 2D Still-Image Face Recognition Algorithms; and the Performance of Face Recognition Algorithms on Compressed Images are the most relevant.

The Multiple Biometric Grand Challenge (MBGC) workshops (2008 and 2009), where the focus was more on the overall technology challenges than on individual facial recognition algorithms is also a relevant document, along with an algorithm study sponsored by NIST in 2006 Face Recognition Vendor Test (FRVT), which also included results from the Iris Challenge Evaluation (ICE) studies. These studies were scientific in nature and were designed to compare and contrast the effectiveness of various algorithms under controlled and uncontrolled circumstances. NIST conducted tests in 1996, 2000, 2002 and 2006 on the subject of Face Recognition. Though these documents are rather clear that the technology has dramatically improved since 1996 in reducing the error rates, there was no clear winner when it came to judging the best algorithms.

Colorado State University Facial Recognition documents

Colorado State University Study – The Computer Vision Group at Colorado State in Ft. Collins, Colorado was engaged in Face Recognition

projects, using Open Source code. In 2010, they released a new Face Recognition Evaluation System (version 5.1) algorithm but they warn it was designed to be used in the MAC 10.6 operating system, which is not industry standard. The original system was released in 2003 (version 5.0). This system was created to evaluate how well face identification systems perform and not to be used as an off the shelf face identification system. Therefore, it has no relevance to the TACIDS grant. A 2010 update to the Colorado State University website: http://www.cs.colostate.edu/evalfacerec/news2010.php explains that their face recognition evaluation site has not changed much since its release in 2003 and they acknowledge and stress that much work has been done (in general) in this field within the past decade.

Open CV (Computer Vision) library reference manual

OpenCV – The Open Source Computer Vision library was developed as a mechanism for software development, where one of the components deals with Face Recognition. It can provide a starting point for developers to create products for PC's. Intel Corporation published an OpenCV Reference Manual in 2000. For the purposes of this grant, Open Source is not a viable option for developing a Law Enforcement Face Recognition product in-house. Research into the topic concludes that much development has already taken place and advanced software has already been produced and implemented for the Law Enforcement community by several vendors who have spent many years and staff-hours accomplishing this. ARJIS is not in the position of starting this effort from scratch.

TACIDS MARKET RESEARCH PROCESS:

The process of research for the TACIDS (Facial Recognition Software) market survey consisted of various searches using keywords and phrases on the commercially available search engines such as "Google" and "Yahoo." Keywords such as ***facial recognition software, biometric technologies and law enforcement*** were utilized in the search for vendors who offer biometric (specifically facial recognition software solutions) for law enforcement. Links found in the results from a keyword search on a search engine were used to find information about various vendors that appeared to fit the criteria for this market analysis.

Any and all vendors found were included in the study, unless it was clear that their solution offered no nexus to Law Enforcement applications. Facial recognition products

that were developed for law enforcement agencies or were being utilized by law enforcement agencies were highly preferred as they are directly advantageous to the research.

Upon entering a vendor's web page, the first action taken in the research was locating any information about the vendor's product/products in the form of "white papers" or any other complete form describing completely the product's capabilities (product brochures included). Secondly, if information was not available in such a complete format, the site was searched thoroughly for any and all data relating to the study. All links on the vendor's web site were searched regardless of their relevance to the study for any applicable information. Finally, when little or no information was available on the vendor's web page, the site was searched for any contact information. (See attachment A for a list of the web sites)

Vendors were contacted via *email* and/or *phone* as well as through submission forms for either additional information on their product or information about their product that was lacking in the research study. Based on contact information obtained, the following text was included in an e-mail to all of the vendors, effectively soliciting specific information about their product/s and/or capabilities.

Market Research for Facial Recognition Platform with Mobile ID Application

The Automated Regional Justice Information System (ARJIS) agency, located in San Diego, CA is interested in building a facial recognition platform, accessible via Web services and searchable (1 to1 and/or 1 to many) from mobile PDA or smart phone application.

We are in the initial stages of market analysis to help determine the best approach, using the best of breed technology to accomplish this task. ARJIS hosts a Cal-Photo mugshot database that contains more than 1 million images, ranging from 30KB to 490KB (JPEG).

Your company has been identified via Internet and other references as a possible candidate for consideration as a service provider for this project.

Could you please take a moment to answer the below listed questions and if interested in this project, please provide the best contact person within your company?

Thank you in advance.

1. *Do you offer Law Enforcement specific biometric products?*

2. *Are your products (a) developed in-house; or (b) are you a reseller?*

3. *Do you offer Facial Recognition searches within your suite of products?*

4. *If yes to #3, does your solution provide (a) forensic workstation; (b) mobile application or both?*

5. *Is your facial recognition search engine (a) Web based; (b) Mobile client based or both?*

6. *Do you offer a software development kit for the (a) Facial Recognition enrollment database and search engine; (b) Mobile search application or both?*

7. *Assuming an image store that contains 2 million photos, can you estimate the time it takes for each search to generate and return a ranked list of similar images?*

8. *Using the same metric as item #7 above, how many searches per hour can your search engine process?*

9. *Please describe your pricing model (licensed per enrolled image, flat rate for server installation, other).*

10. *Do you support multiple Facial Recognition algorithms?*

11. *Please list one or more of your largest, most successful Law Enforcement implementation that utilizes Facial Recognition.*

12. *Please describe your approach (in general terms) to building a Facial Recognition platform against the existing ARJIS image repository.*

13. *Please describe your approach (in general terms) to providing a mobile solution for searching the facial recognition database and returning a list of potential matches to an officer in the field. The approach can include a completed (COTS) product or a software development kit for use by ARJIS developers.*

Thank you and I look forward to your response,

The above survey questionnaire was sent to the following companies:

- Dataworks Plus

- Cognitec
- L-1 Identity Solutions
- Imageware
- Cogent
- OmniPerception
- Sybernautix
- Neuro Technology
- MorphoTrak (Safran Group)
- Animetrics
- Airborne Biometrics Group

Answers to the survey questions can be found in the Market Survey tab of the enclosed "Facial Recognition Software Companies" spreadsheet.

On receipt of the completed questionnaires, a set of sample photo images (jpg files) was sent to each vendor, asking that they do an in-house evaluation as to the viability of the photo repository that ARJIS hosts. This repository represents copies of booking photos captured within the San Diego County detentions system and is known as the ARJIS Cal-Photo Node. A mutual non-disclosure agreement was executed with each company to ensure that the photos were used only for the intended purpose and that they were not to be distributed outside of their company.

The following text was sent to the vendors along with the sample files:

Thank you for your continued interest in the ARJIS facial recognition project. Attached is a zip file containing 104 photo images ranging from 42KB to 140KB in size. Please let me know if your organization does not allow zip files through your e-mail system and we'll work out another approach.

As stated earlier, these images are provided as a mechanism for your staff to determine whether the quality of these images is sufficient for enrollment and subsequent matching within your environment.

I would appreciate a response within two weeks of receipt of this message and photos, along with a list of those images (by file name) that do not work within your system and an overall assessment of the images as a whole.

Thank you for your efforts,

SITE VISITS AND PRODUCT DEMOS

In addition to the product demos that were available on company websites, several vendors (due to their proximity to San Diego County) were able to provide product demos. ARJIS visited several companies and was also able to attend a meeting in which various products were demonstrated to include:

- *L-1 Identity Solutions (formerly Identix, formerly Viisage algorithm)*
- *Los Angeles County Sheriff's Department (Cognitec algorithm)*
- *Dataworks Plus (San Diego Sheriff's Department - Cognitec algorithm)*
- *Cogent Systems (Pasadena, CA)*
- *Airborne Biometrics Group, now known as Face First, LLC (Cognitec algorithm)*
- *Coplink Face Match (formerly Visiphor)*

RESEARCH FINDINGS:

The attached Spreadsheet B includes the responses from the market research and the results of the viability assessment. Below is a summary of the aforementioned product demonstrations.

L-1 Identity Solutions – ARJIS was introduced to the L-1 sales representative through a trusted and respected member of the San Diego Sheriff's Department who was interested in forming an alliance for new technologies related to biometric identification. This resulted in several meetings (to include a company systems engineer). Ultimately, the sales representative brought a demonstration system to ARJIS, where he demonstrated the enrollment process (using a couple of the ARJIS sample images). He then demonstrated the matching capability against a relatively small database that was resident on his laptop. He claimed to have several large-scale customers and specified Pinellas County, Florida as the model agency for his product. ARJIS contacted a representative from Pinellas County who confirmed that the product is working very well.

Los Angeles County Sheriff's Department – An ARJIS representative accompanied two San Diego Sheriff's representatives to Los Angeles County to witness a demonstration of their mobile application that utilizes facial recognition (Cognitec algorithm). Their system is customized so that a field deputy can use the mobile (cell phone) application to capture a photograph of a subject in the field and transmit it via secure e-mail to the back-end system, where the matching occurs. The system will return up to 5 potential matches, along with a link to a separate application to actually check the results. Los Angeles County representatives were quite happy with their application and the performance of the Cognitec search engine. The San Diego Sheriff's Department was interested in this demo because they were using a DataWorks Plus algorithm in their

eMug system and at that time they were in the process of evaluating a potential upgrade to Cognitec. They have since instituted that upgrade.

DataWorks Plus – The San Diego Sheriff's Department has been using Dataworks Plus for facial recognition and there have been concerns with the product's performance. ARJIS staff was able to view a demo of their system and it failed to locate a match (using the same photo as that of the enrolled photo). Since that time, San Diego has decided to go ahead with the Cognitec upgrade, which has been proven to provide increased performance.

Cogent Systems – ARJIS staff accompanied a representative from the San Diego Sheriff's Department to a pre-arranged visit at Cogent Systems, located in Pasadena, California. This demonstration was well orchestrated and included key staff members and developers to answer relevant questions. Cogent has recently won the contract to replace the existing AFIS database at the San Diego Sheriff's Department and while they admitted that they are rather new to the facial recognition aspect of biometric identification, they claim to have a viable product. They did a live demo, using an ARJIS staff photo as an example for enrollment and matching purposes. The mobile application was not yet mature. There was no authentication method in place but the matching component worked as advertised.

Airborne Biometrics Group Face First – The company president and local representative from Airborne Biometrics Group (located in Camarillo, CA) brought a live demo to ARJIS. This was by far, the most impressive demonstration to date. The demo consisted of the following: 1 fixed video camera (CCTV); 1 laptop w/server side application and database on local area network with the camera; 3 different cell phones. The representative took an ARJIS staff member's photo with the cell phone camera. The photo was electronically sent to the backend database where an attempt to find a match was made. Finding no match, the application on the phone indicated to the rep that this was a "new" person. The rep collected bio information and in effect, enrolled the photo (along with the incident data and alert subscription) into the database. Next, the rep had the staff member walk in front of the fixed CCTV camera. As he did, all present noticed that the laptop screen (showing the live video from the camera) locked on the staff member's face and found an immediate match from within the database, displaying the original image plus the current one side by side. At the same time, an alert was sent to the rep's cell phone, telling him that the system had found a match based on the CCTV camera. The product name is Face First and the algorithm used is Cognitec.

Coplink (i2) – FaceMatch - A conference call was initiated between ARJIS and Coplink staff, utilizing a live web-meeting. ARJIS already utilizes Coplink in a production environment for all of its customers. The "FaceMatch" component is an add-on feature of the existing Coplink Detect product and is tightly coupled with the existing search capabilities on persons. Coplink (i2) purchased Visiphor and its proprietary algorithm in the past year or so. They are currently implementing their "FaceMatch" component in

Orange County at this time. They demonstrated FaceMatch on a test database but in their current version of Coplink Detect. It appeared as a sub-tab of the Person search. This allows for standard biographic filtering while simultaneously submitting a probe image for comparison. It's as simple as dragging and dropping or browsing for a jpg image into the Coplink FaceMatch photo frame. When the search is executed, the user sees different images quickly superimposing in the lower right corner (much like a CSI TV show) and then similar images with probability scores are displayed in a gallery where the officer can review each one and then select for more detail. Once selected, the user is presented with the standard list of incident documents and associations for that person. Additionally, ARJIS and Orange County are already connected node to node and these searches can be executed across nodes.

Pinellas County Sheriff's Office, Florida – Facial Recognition System **-** One of the law enforcement leaders in facial recognition systems is the Pinellas County Sheriff's Department. They have a very robust system with several law enforcement partners, including Miami-Dade police and the Florida State DMV. They have been using L-1 Identity Solutions (Viisage algorithm) for several years. It is used to capture mug shot images during the booking process and is probed from desktop and mobile applications. The ARJIS TACIDS project manager witnessed a live demonstration of this product during an Nlets working group meeting in Chicago. A captain from the Pinellas County Sheriff's Office gave the demonstration, adding that they have been using this technology for about ten years and that they have several success stories compiled.

Of all of the proprietary facial recognition algorithms researched, there are four that appeared to have the best chance for success within the ARJIS environment:

- ✓ **Cognitec**
  - Currently used by Los Angeles Sheriff, San Diego Sheriff and endorsed by Airborne Biometrics Group
- ✓ **L-1's Viisage**
  - In use at Pinellas County, Florida and Pennsylvania State Police among others
- ✓ **Cogent**
  - Relatively new to face recognition but is a California company with much experience and a great presence in biometric identification (primarily fingerprint identification).
- ✓ **Coplink's Visiphor**
  - Unique in that the Face Match module is built into the existing Coplink search interface, where a match on a face yields identifiers that are already linked to incident data contained within the Coplink database. It is also capable of doing node to node searches.

During the course of this research, ARJIS has learned that there are several different purposes for face recognition software within the law enforcement environment. Here are a few examples:

1. Field identification of persons through one to many matching against photo repository

2. Forensic identification of unknown person/s from surveillance photos

3. Inmate tracking within a detentions system using face recognition

4. Mitigation of ID Card and Driver's License fraud using face recognition

5. Proactive alerting of known criminal and "watch list" persons via live video

This research focused on the first example (field identification) but because ARJIS is actively engaged in a proactive alerting effort (Officer Notification and Smart Alerting System) and Field Interviews (otherwise known as Suspicious Activity Reports), several of the examples apply.

IMPLICATIONS FOR POLICY AND PRACTICE

ARJIS also tackled the complex FBI CJIS requirements in the use of wireless devices as related to sensitive law enforcement data. Since Android was the operating system of choice for this project, ARJIS took several steps in order to be in compliance.

- ✓ The Samsung tablet devices were "rooted" and a secure firewall was installed and activated.
- ✓ The device wireless service was routed from the carrier directly to the ARJIS domain via Sprint Data Link and static IP.
- ✓ Anti-virus protection was installed and enabled.
- ✓ Remote device management software was installed and activated, allowing ARJIS administrators to secure, locate, monitor and otherwise manage the devices as necessary.
- ✓ Access to the applications is via Juniper secure VPN with high level encryption.
- ✓ Advanced Authentication was enabled when accessing the VPN. This was accomplished through SecureNet 2-factor token access.

MOBILE APPLICATION TECHNICAL APPROACH

The initial technical approach to building a facial recognition platform and mobile application was to utilize the information gained as a result of the market analysis plus the various

product demonstrations to form a strategic functional requirements document. This functional requirements document was transformed into a formal "Request for Qualifications" and was advertised to the biometric development vendors. This RFQ process resulted in a short list to include Cognitec, Dataworks Plus and Airborne Biometrics Group (now known as Face First, LLC). After reviewing each of the three companies' responses the RFQ team, which consisted of ARJIS and San Diego Sheriff Department (SDSD) staff, Face First was selected to develop the custom application with back-end process per the ARJIS specifications. Reasons for this choice included, the high cost of licenses for one of the company's mobile device licenses (more than the equipment funding awarded in the grant), and one of the recommended solutions didn't fit in the ARJIS environment. Face First, LLC was the most willing to develop a custom application at a reasonable price, as opposed to selling an existing commercial off the shelf product.

ARJIS still needed an algorithm, so Face First and ARJIS negotiated with Cognitec to acquire licenses for FaceVACS, which scored favorably within the market analysis and had shown success in other law enforcement platforms. Face First was tasked with building a back-end process to handle the requests and responses from the TACIDS application on the mobile devices (in this case, Android tablets and phones) and to customize their existing Face First application to ARJIS specifications. Face First was also tasked with adding functionality to allow users to create field interview records, complete with the photo images, biographical and incident data captured in the field and then make the data available for upload to the ARJIS Enterprise database.

DATA SOURCES

ARJIS receives mug shot records from the San Diego Sheriff's Department booking system entitled eMUG. These records are sent via ARJIS web service to the ARJIS Cal-Photo database where more than 1.3 million records exist (dating back to 1995). In addition, ARJIS has approximately 93,000 mug shot records that were extracted from the Chula Vista Police Department's booking system entitled Offender Track.

It is a desired goal for the ARJIS TACIDS mobile application to directly access the eMUG system through a web service at some point in the future. For this effort, TACIDS will utilize the ARJIS Cal-Photo database.

On a parallel project, ARJIS added a facial recognition component to the existing Coplink system entitled FaceMatch. This system utilizes the Visiphor algorithm which is now owned by Coplink. ARJIS will be conducting side by side comparisons between TACIDS and Coplink FaceMatch to evaluate performance and successful field identification incidents.

MOBILE DEVICE SELECTION

Since the wireless program inception in the early 2000's ARJIS has rolled out multiple devices to users in throughout San Diego. For this project, it was important that the devices we installed TACIDS on had a suitable camera. With so many options available currently available, the decision was made to select a sample of devices, field test them, and survey the field-testing participants.

Eight devices that ARJIS had previously acquired were selected for field testing.

HTC Evo 4G
Samsung Galaxy Sll Epic 4G touch
HTC Evo Shift 4G
Samsung Nexus S 4G
HTC EVO 3D
Samsung Galaxy Tablet SPH-P100
HTC PC515 Tablet
IPhone 4

Field testing participants were selected by law enforcement specialty and availability.

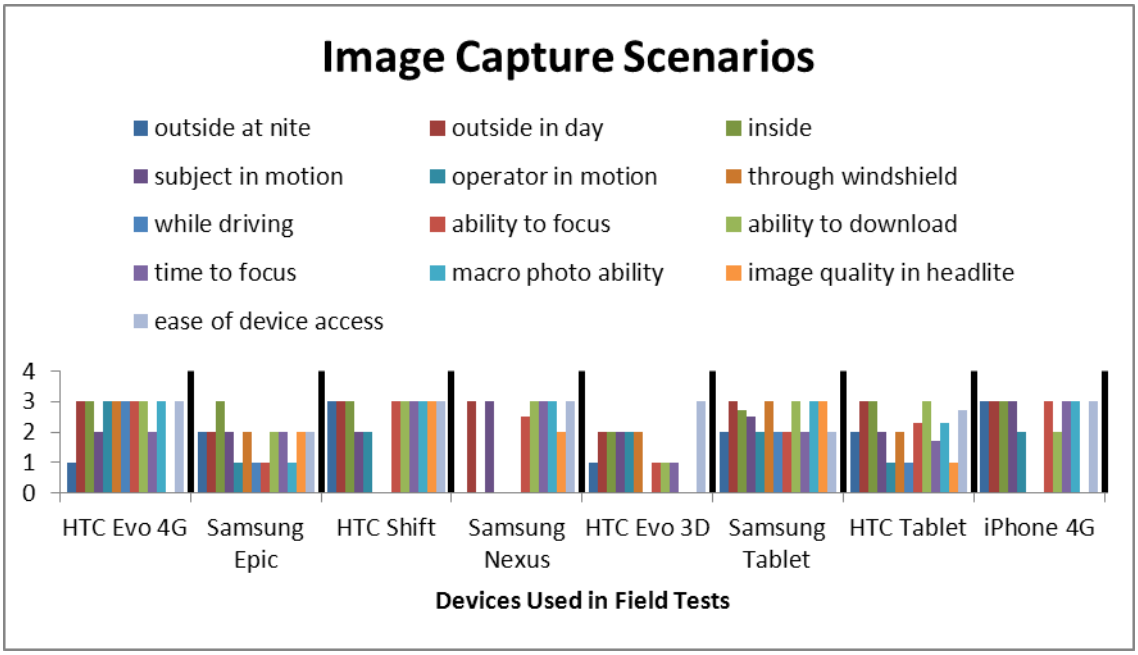
North County Regional Gang Task Force
Escondido Police Department Gang Task Force
National City Police Department
California Border Patrol
US Immigration and Customs Enforcement

The evaluation had three components which were developed by ARJIS and ICE representatives. A survey was created to assist in determining the current methods for accessing and capturing images. An evaluation matrix was developed to assess various functionality requirements as well as the image quality of the devices. There were several focus group meetings to obtain feedback the various devices.

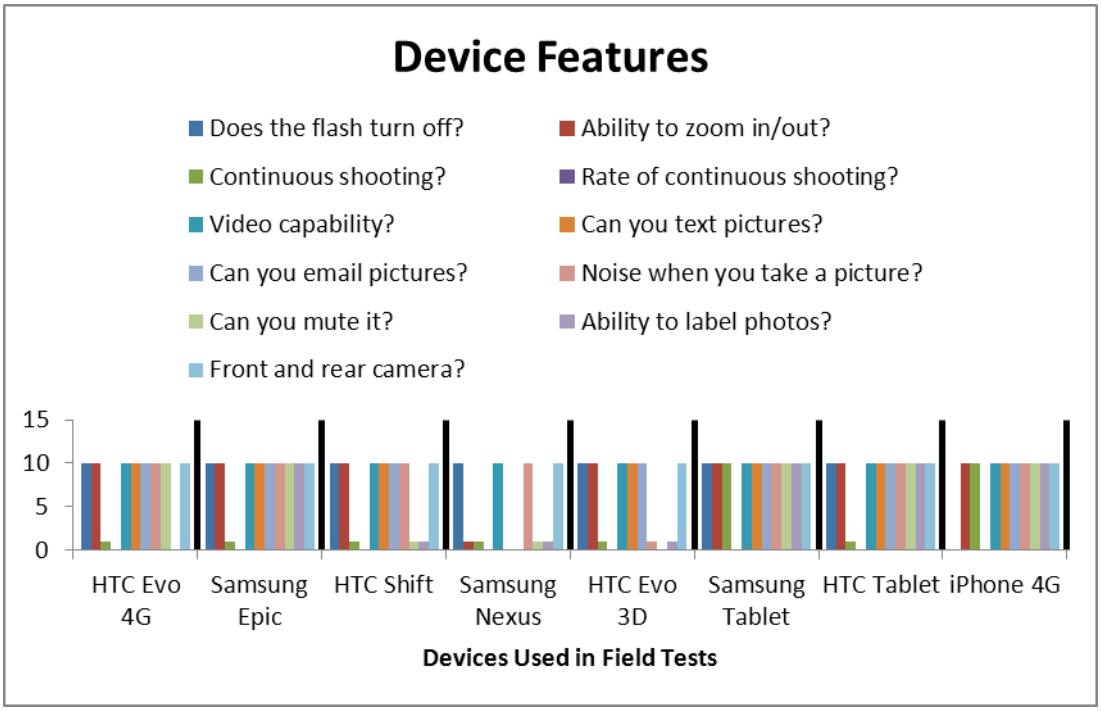
There were two sections in the survey. In the section on image quality, survey respondents captured over 1800 images. Respondents rated the images (poor, satisfactory, excellent) in thirteen categories:

- Photos taken outside at night

- Photos taken outside in the day
- Photos taken inside
- Photos taken while subject is in motion
- Photos taken while you are in motion
- Photos taken through a windshield
- Photos taken while driving
- Ability to focus on your target
- Time and space it takes to download photos to your machine
- Amount of time it takes to focus
- Ability to take macro photos (close up such as a scar)
- Images taken in artificial light (in the field with car headlights)
- Ease of accessing device (too big to carry in pocket)



In the second section of the survey, device features that had been identified as important were rated by the participants.



Based on the survey results and the feedback from the user groups, ARJIS determined that the devices best fit for the TACIDS effort would be Samsung tablets. Through another effort ARJIS had deployed 250 tablets to the regions Terrorism Liaison Officers (TLOs) which will serve as a great test bed for TACIDS.

Security Requirements

When ARJIS began to implement applications for PDAs and Smart Phones, the operating system of choice was Windows Mobile. Since that time, technology has changed dramatically and the market has driven the cellular carriers to standardize on Android and Apple IOS based devices. Because Apple is not FIPS complaint and to ensure we are following FBI and Cal-DOJ Security requirements the ARJIS devices use the Android Operating system. There was a significant amount of work that went into ensuring the devices and the operating systems met FBI CJIS and Cal-DOJ security

The ARJIS internal technical framework for wireless devices was established to ensure usability from an end user stand-point, while maintain complete security and management of the device. The framework mirrors CJIS requirements for ensuring both the physical and network security of the devices. The ARJIS framework was extensively tested and consists of the following metrics:

- The device security must not interfere with the functionality of the device.

- The device must be configured to deny the ability to store potentially sensitive data physically on the device.
- The device must meet CJIS criteria for Firewall, Encryption and Virus Protection.
- The device must use COTS (Common off the shelf) software to keep costs low.
- The device must be remotely manageable, and the device configuration must be protected against changes and unauthorized configurations.

CJIS security requirements specifically state that any device which connects to a law enforcement network must meet the following requirements:

- FIPS 140-2 Encryption Standards
- The device must have a configurable firewall, able to block ports and be managed.
- The device must have a management utility for remote management.
- The device must have virus protection.
- The device must have a screen lock password, enabled upon start-up.

The ARJIS Samsung devices have been approved as FIPS 140-2 compliant devices per the manufacturer, which is why they were specifically chosen for our project. To meet CJIS requirements, we installed an all-in-one product called AVAST that provides us a user configurable firewall, virus protection and anti-theft as well as encryption features. We have hand configured each device to be exact with specific applications and ports blocked. We also have secondary virus protection software called JUNOS installed on the devices to ensure maximum protection.

The ARJIS software is web based, and we have configured the devices web browser to clear all cache and data upon exit, and wipe it from memory. Connectivity to the ARJIS web applications requires the use of a two factor VPN token, which provides secure communications over the wireless network.

In addition, to meet the remote management requirements, we use a product called MobiControl that allows us to control any device remotely, update its configuration and shut it down remotely if required. We are exploring other products that will enhance this functionality.

Upon boot, the device is immediately sent to screen lock, where the user is required to enter a password. Every time the device times out or goes into power saving mode, upon waking up the device requires that password to be entered again before use.

While we were required to ROOT the device to install the firewall, we use the same AVAST protection software to lock down the Super User permissions, preventing

unauthorized administration of the device. We also successfully reset the ROOT password for the devices with a hardened password for ARJIS.

Rooting the devices was an extremely labor intensive task mainly because we had to take the standard carrier Android version on the device and recompile the OS, injecting the Super User ROOT application. While there are multiple ROM's currently available for the devices that are already rooted, we could not take a chance that any of the publically available ones contained bugs or issues or were already compromised.

Each device also had to pass specific validation testing, including the testing of the firewall application against known exploits, as well as purposely exposing the device to malware and viruses to ensure the device responded accordingly. In configuring the anti-theft, we were able to mask the device's Super User access, encrypt the administrator password and set security policies on the phone directly to ensure that the phone is wiped upon configured triggers.

The final security feature is the use of a direct VPN connection with our chosen wireless carrier, Sprint. All wireless devices have an ARJIS assigned internal IP address which Sprint routes directly to us. Regardless of where the device connects on the Sprint network, all data traffic is routed through the secure ARJIS connection with Sprint, directly back to ARJIS for both Internet and VPN communications, meaning the device also passes through the ARJIS Network Proxy and Firewall servers directly.

The current frame work and solution, while still a work in progress, is specifically designed to be Android device agnostic, meet usability requirements and CJIS requirements for security. We are also looking to collaborate with other agencies to refine additional security features and policies to help shape future mobile device security policies. ARJIS is also exploring additional remote management and security options to further enhance our mobile devices.

FUNCTIONAL GOALS AND REQUIREMENTS

TACIDS is a modular software solution for Law Enforcement field personnel, using facial recognition technology. The primary purpose is to facilitate and/or verify the identification of individuals encountered by Law Enforcement officials in the field when other more traditional means are not effective or available. In order for this technology to work, several requirements needed to be met.

- Identify one or more photo image repositories (database) available to ARJIS to include identifying demographics for each image (name, address, date of birth, driver's license number, FBI number, AFIS number, etc.)

- Identify and procure the “best of breed” enrollment and search algorithm.

- Successfully enroll all available photo image records into the TACIDS database.

- Implement a search engine capable of searching several million records at a time efficiently, based on programmable thresholds and parameters. This database and search engine must be portable and extensible.

- Build a web service (service oriented architecture protocol), attachable to an Enterprise Service Bus that allows one or more user applications to access the database for enrollment and search purposes.

- Build a GUI user application for the desktop workstation (web-based) for enrolling and searching the TACIDS database via the web service.

- Build a mobile application for smart phone or tablet (as device operating system agnostic as possible) for enrolling and searching the TACIDS database via the web service.

Function List

Functional ID	**Component**	**Sub-component**	**Functional Requirement**
1	TACIDS Database	Photo Category	The TACIDS database must be able to differentiate whether the enrolled photo is a mug shot photo (based on verified ID) versus one enrolled under different circumstances (Field Interview, Surveillance Photo, etc.). This will be handled via a “photo category” field in the database.
2	TACIDS Database	Record	At minimum, the database (in

		Demographics	addition to the digital photo template signature) must include or be linked to a sufficient number of fields for inclusion of cross-identifying demographics. These include but are not limited to: Last Name, First Name, Middle Name, Date of Birth, Address(es), Phone(s), FBI number, Driver's License number, Social Security Number, State ID Number, AFIS number, etc.
3	TACIDS Database	(SQL Server 2008 or later) Indexed and Tuned	The TACIDS database must be structured within the SQL Server (version 2008 or later) environment and must be indexed and tuned so that several million records can be searched within 30 seconds or less.
4	TACIDS Database	Enrollment Services	There will be a mechanism for enrolling large batches of existing images, effectively building digital templates specific to the chosen facial recognition algorithm for each image.
5	TACIDS Database	Enrollment Services	There will be an ongoing enrollment system for all new image records entering the TACIDS database via interface ingestion from other systems or direct enrollment.

6	TACIDS Search Engine web service		The search engine must be a web service, using Service Oriented Architecture Protocol that is capable of using a digital photograph and/or demographic search criteria to search the TACIDS database and return a specified number of potential candidate responses (based on programmable threshold parameters). The responses will be returned to the user application for further action.
7	TACIDS Search Engine web service		The web service will receive information from the user applications to perform enrollment services, based on one or more captured photographs and accompanying demographic data.
8	TACIDS User Application	Mug Shot Interface	Mug shot images received by ARJIS into the Cal-Photo node will be enrolled into the TACIDS database via automatic interface. These photos and accompanying records will not be editable through the user application.
9	TACIDS User Application	New Record Enrollment	The TACIDS user application will contain a module allowing authenticated users to enroll new photo records, along with specified demographic and

			incident-related data. These records will fall into one or more different categories (other than Cal-Photo mugshots).
10	TACIDS User Application	Search Mechanism	User will be able to search the TACIDS database by submitting a copy of a digital image, along with additional search criteria. These criteria will not be mandatory, but must include specific input that could effectively narrow the search by items such as: Photo Category (Field Interview, Mugshot, Other Incident Record); Last Name, First Name, Approximate Age, Sex, Race, Residence Address, Crime Potential, etc.
11	TACIDS User Application	Search Mechanism	If the system fails to locate a match (as verified by the person conducting the search), the user must be provided with the opportunity to enroll the new image into the TACIDS database and the new record will be categorized as a field entry.
12	TACIDS Mobile Application		The TACIDS mobile application must be able to capture and utilize the functionality of the smart phone's built-in camera as part of the application.
13	TACIDS Mobile Application		The TACIDS mobile application must allow for the submission of a photo image captured in the field to the TACIDS search

			engine. A list of potential match candidates will be presented to the user, in ranking order (high to low priority) based on the threshold set at the server. Defined biographical data will be presented to the user, along with the corresponding match probability score.
14	TACIDS Mobile Application		In addition to the capture ability, using the smart phone's onboard camera, the TACIDS mobile application must provide a mechanism to attach an existing, locally stored JPG image for submittal to the search engine.
15	SRFERS Integration		The TACIDS mobile application functionality must be written in modular form, so that it can be easily integrated into the existing SRFERS mobile application. This will allow for recursive status and incident-based queries of TACIDS search results without the need to switch applications and re-enter the search criteria.

ACCESS CONTROL & AUDITING

User authentication and authorization uses the ARJIS Security Center (LDAP to Active Directory) but also has its own configurable security module for entities that do not utilize LDAP. The TACIDS Engine will manage items such as:

- Login security parameters (password complexity requirements)
- The number of login attempts before lockout

- The TACIDS Engine also provides full audit and audit reporting capability

ERROR HANDLING

The TACIDS Engine also analyzes and provides feedback to the user on items such as:

- Whether certain data sources specified in the queries are unavailable
- Timeout parameters per data source
- Indication to the user as to the status of each data source searched (in-process, complete, etc.)
- System error messages

TACIDS OUTCOMES

IN 2011, through a partnership with the Department of Homeland Security, ARJIS deployed 250 Samsung tablets equipped with access to ARJIS applications to San Diego County Terrorism Liaison Officers. Because this group was familiar with the ARJIS Wireless Program, Samsung tablet functionality, and is comprised of officers from multi jurisdictions, it was recommend a selected group of twenty would serve as the TACIDS test and user group. The users with the highest usage and those who had provided the most feedback to ARJIS were selected. The group, which consisted of police officers, agents and deputy sheriffs was introduced to TACIDS, and then trained on the use of the system. Immediately after the TACIDS application was made available for users to test, ARJIS received feedback regarding the value the tool brought to the law enforcement community.

News of TACIDS spread quickly and ARJIS users from across the region were requesting access to the application. The demand for TACIDS became even more evident after the system was presented to the ARJIS Chiefs Sheriffs Management Committee. The Committee was impressed with the applications functionality and the potential time savings it would provide their agencies.

While many of these agencies already had Samsung tablets, some were using Smartphones. At the agencies request, TACIDS was implemented on Smartphones. ARJIS was able to ensure that the functionality of the application remained the same and CJIS security requirements were still able to be met. This allowed ARJIS to expand the TACIDS user base; in turn new users were tasked with utilizing the system during routine tactical operations and to report any and all feedback related to the system.

This access greatly assisted ARJIS with testing the TACIDS application. Because individuals must have an existing photo enrolled in TACIDS, testing with live data was difficult. By providing Immigration Customs Enforcement (ICE) agents with access to TACIDS, tests were able to be conducted with live data. The majority of the time

undocumented persons are detained by San Diego officers they are sent to the SDSD jail, and then transferred to ICE Detention Centers. During the local booking process their mugshots are captured and uploaded into the SDSD eMug system, the same data course TACIDS utilizes.

By providing ICE Detention Center agents with access to TACIDS, they were able to take individuals who had been brought from the SDSD local jail out of their cells and capture their images. The images were then run through TACIDS to determine if the photo lineup returned to the agent would include the recently captured local SDSD mugshot image. This process was very helpful in validating the TACIDS functionality and in ensuring that it was able to return matching images.

ARJIS received a variety of success stories which were helpful in validating the effectiveness of the application. In addition, user meetings were held to identify enhancements they felt would be useful in the future. Below is a sample of success stories and feedback provided by TACIDS users.

SAN DIEGO REGIONAL FUGITIVE TASK FORCE

- "I just wanted to send a positive note on two events regarding the new TACIDS program. Three tablets were upgraded with the test program last week. The very next day we used it on our first call. The residence we were in was a known flop house with several occupants. One male ran out the back into the garage to hide but was located and detained. The male was photographed and entered into the TACIDS system. A 99.97% match was provided on the male. A records check of the name and DOB provided the male had an active felony warrant and was a parolee at large. – San Diego Regional Fugitive Task Force"

- "On 08-23-12 the task force conducted a high risk contact on a residence with a sighting of a parolee at large entering. The residence was entered and cleared finding several occupants inside. The parolee at large gave an incorrect name to officers. The TACIDS program was utilized and a match of 99.97% of the photo was given. A 4th waiver search also found a loaded handgun where the parolee was hiding."

- "In five days of utilizing the system three arrests have been made and several photos have been updated. One 10 minute new update was created with a new photo."

- “During the annual "XXXXX" Operation, a male was contacted and gave a false name to the Deputies. The ARJIS tablet was used and a positive identification was made on the subject using TACIDS. The subject had three active felony warrants for theft and several pending case throughout San Diego County for storage unit theft.”

- “Deputies conducted a traffic stop on a vehicle. A male passenger had no identification and gave a name the deputy believed was false. I was contacted and advised the field units to send me a picture of the male. The field picture was downloaded into the TACIDS program. The first picture I received showed the subject with his eyes closed and slightly looking down. I had the units send me an additional picture and l attempted to enter the current photo. The TACIDS program still gave a positive hit on the subject in the 70's of confidence. The 2nd picture I received was of good quality with open eyes and no shadowing. I received a 98% on the confidence level. The subject was arrested without incident. Additionally the subject was actively being sought after by the San Diego Regional Fugitive Task Force as a possible armed and dangerous Parolee at Large. The ARJIS tablet again was a resource on and off the field to identify wanted fugitives and place them in jail without further incident.”

- “I received this picture for ID on the TACIDS program. Suspect was very uncooperative and was positively identified by the sent photo to tablet. Suspect was an AB109 former parolee and a Vista Homeboy gangster. His new charges will be driving a stolen vehicle, felony hit and run and felony evading. Just thought I would send another success story.”

Immigration Customs Enforcement

- “This is the most awesome thing EVER!!! We went over to the holding cells this morning to try out the TACID software. Pulled out three aliens who were recent jail releases. Took pictures and let the machine do the rest. Hit with 99.6% on two of them, and the third was at a 68%, but it identified all of them.“

- “Today while conducting warrant services in Oceanside, we made contact with the neighbors of a subject we were looking for. As we were talking to the individuals who lived next door, our "spidy senses" were tingling. So this neighbor became the focus of a field interview. The subject was being evasive answering our questions. it was determined that the subject was in the United States illegally so we arrested him for that. I decided to transport the subject

downtown, still not knowing exactly who I had in custody. While driving him to jail, I prodded a little more and the subject stated that in 2003 he received a conviction for DUI in San Diego and that was the ONLY time he was arrested. So I whipped out the Droid and snapped a quick photo and submitted for search. The subject looked inquisitively at me not knowing the truth was only 8 seconds away. I received a match of 99.96%. This revealed several prior arrests and convictions and provided me an FBI #. When I showed him his booking photo, his jaw dropped. Thanks again for the opportunity to evaluate this device."

National City Police Department – Homicide/Gang Unit

- "Just wanted to drop you a note on how the facial recognition worked yesterday. Right after our weekly investigations' meeting I was assisting other detectives on a follow up of a kidnapping / robbery. We ended up at the suspect's house and contacted numerous people. I contacted two people who were not involved but were in the suspect's apartment. One had ID and had a Parolee at Large warrant and was immediately arrested. The other person, a female, had no ID and gave the name of a real person in AZ. It was obvious this female had been arrested before but the record's check showed no hits of a criminal record. At this point in the investigation she was not a suspect in the kidnapping and we did not have anything else on her….we knew she was lying about her identity and were running out of detention time. I sent another officer on my team who had TACIDS on his Smartphone the photo of her and within a couple of minutes we had her identified and learned she was a parolee at large. She was arrested for the warrant and identity theft…very helpful tool."

San Diego Sheriff's Department

- "On 10/5/12 at about 1750 hours, Vista Traffic investigators responded to a report of a hit and run collision in the parking lot of location 1. The vehicle involved was subsequently stopped in a nearby subdivision. During the investigation, a male subject who was driving the vehicle at the time of the traffic stop verbally identified himself as David "suspect one". A record check was unsuccessful in locating a driver license or any other information about him and he was cited. He provided a thumbprint on the citation and was photographed prior to being released."

- "On 10/6/12 an ARJIS analyst Muenzer was emailed a photo of "suspect one" and his two companions. Analyst Muenzer ran the photos provided through the TACIDS tablet and then Coplink Face Match. The programs resulted in a possible match of "Mr. XXX". Both systems yielded Mr. XXX as a high confidence match. On 10/11/12 Deputies from the Vista Gang Enforcement Team located the motor home involved in the original incident. Mr. XXX was contacted inside the motor home. Mr. XXX again identified himself as suspect one. Upon being presented with a copy of a previous booking photo, Mr. XXX admitted his true identity he was subsequently booked on a felony warrant."

- "I have been working day shift in the Lemon Grove / Spring Valley area. We switch to nights on 10-20-12. I have used the TACIDS on about a dozen subjects who were stopped for violations and were not carrying ID. Subjects either consented to being photographed or were being cited for various reasons. The program has worked 10 of 12 times accurately ID the subject. The other two were believed to not have a previous record. The system has led to arrests for 4 felony warrants and two PAL's. Two other individuals had non-bookable misdemeanor warrants."

- "The team is very happy with the system. They plan to use it more when on night shift and contacts go up. It has been less effective when subject is in partial sun. Either full light or full shadow works best. Holding in panoramic view is more effective than portrait. Can't wait to add the fingerprint module."

The success stories that resulted from TACIDS validated the time savings that facial recognition in the field enables users by assisting them in positive identifications and in the detainment of parolees at large who were not forthcoming with their previous charges. Furthermore the users reported the tool's ability to reduce the frequency of physical force they are often required to use when individuals are being uncooperative. By enabling officers to remain a short distance away from individuals and taking their picture verses having to physically search them for identification or forcing them into fingerprints, TACIDS has enhanced officer safety.

This project also resulted in a recommended set of requirements for implementation of the facial recognition platform in the public safety mobile environment.

  - Wireless devices must be capable of sending and receiving data over a wireless network that meets security requirements. It is also imperative for the mobile devices to have cameras that are capable of interacting with custom software. Fortunately, ARJIS already had a mobile program

in place with a private network, security and remote access support for devices with built in cameras.

- There are three software licensing components required to implement this solution.
  - Algorithm license - the licenses can be costly as they are based on the number of image "enrollments" during the encoding process. In the case of ARJIS, an appropriate number was 2,000,000 images. The encoding process, after the initial run, must have an ongoing process for newly created records.

  - Backend Processing - submission of probe images to the system and provides the feedback to the officers. The back-end solution must be capable of interacting with the mobile application. A database of photos must exist that contains images that are of sufficient quality to be encoded.

  - Mobile and Desktop Client license – these licenses are usually based on the number of devices that utilize the mobile or desktop application.

NEXT STEPS

As technology advances the use of mobile and biometric tools will continue to play a pivotal role in the law enforcement community. ARJIS intends to stay at the forefront of this trend by expanding on these tools as new technologies are developed, and by evaluating those that are already in place.

ARJIS will evaluate the TACIDS program to address topics such as environmental factors, the relevance of confidentially scores and how the software compares to other similar technologies. The evaluation results will be provided to public safety agencies through out the nation who are implementing similar systems.

During this first phase of TACIDS, feedback was obtained on individual's facial expressions and how they affected the confidentiality rates of responses. Users also reported the influence sunlight played on image matching. ARJIS intends to expand on this by addressing other factors such as skin color and the proximity to the individual whose image is being captured.

An agency in Florida using facial recognition does not return confidentiality scores with the associated images. ARJIS was informed that the reason for this was that the agency did not want the scores to influence user's decisions while making positive identifications. ARJIS intends to assess how confidentiality rates were utilized by TACIDS users when making positive identifications.

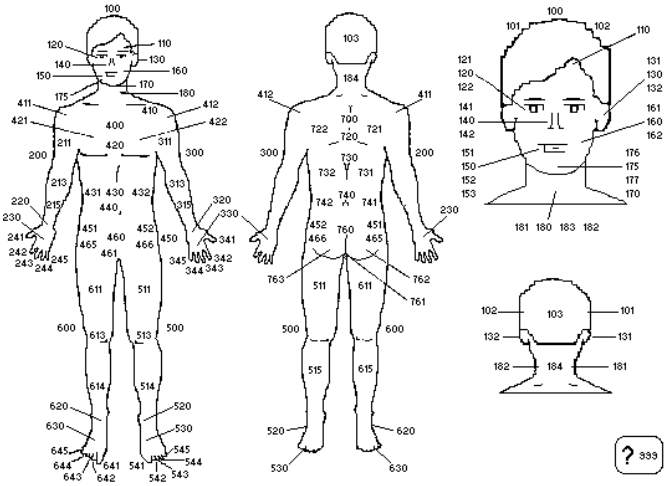
Also planned is to compare the TACIDS software with other facial recognition products such as COPLINK's Face Match. ARJIS has procured and installed this product and is in the process of testing the software. Images will be submitted to both systems to compare the return rates and time.

ARJIS will continue to maintain its partnership with Nlets and the California Department of Justice and will participate whenever new facial recognition data sources become available. The TACIDS solution is staged to allow interaction with other systems through web services, as long as the other data sources can provide sufficient biographical data along with the return list. Potential sources ARJIS is looking at to include: California Cal-Gangs, ParoleLEADS as well as CA Department of Motor Vehicles.

Finally, the FBI and ARJIS are proposing to enhance this tool by developing the ability for users to attach pictures of SMTs to TACIDS records. The images will be accompanied by fields containing selectable descriptions of the scars marks and tattoos. Typically the metadata agencies use to describe SMTs is based on NCIC standard codes. However, these standards are outdated and do not include descriptions such as full sleeved tattoos and gangs which have become much more prevalent over the last decade.

New descriptions will be developed by a team of federal, local and state law enforcement officers, ARJIS, and the FBI. They will be mapped to the existing NCIC codes to comply with national standards. All of the data captured will be stored in the ARJIS incident database and will be available via the ARJIS federated query system known as SRFERS.

Another potential component of this application could be the ability for officers to select the location of the SMT on an individual by touching the area on a body location map (see below). The system would translate the location to the various NCIC location codes (i.e. upper right arm) and would save officers time as there are over 100 SMT location codes to choose from.



CONCLUSION

In conclusion, ARJIS would like to thank the US Department of Justice (Office of Justice Programs) and the National Institute of Justice for the opportunity to research, study and implement this successful mobile facial recognition project. ARJIS believes that this will set the stage and visionary goals for future direction and development efforts toward the ultimate goal of public safety.