AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY

# Can You See Me Now?
# Visualizing Battlefield Facial Recognition Technology in 2035

By
Thomas C Westbrook, Major, USAF

A Research Report Submitted to the Faculty
In Partial Fulfillment of Graduation Requirements

Advisor: Lt Col Terry Bullard

Maxwell Air Force Base, Alabama

April 2010

## Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

## Contents

Disclaimer ………………………………………………………………………………...………ii

Abstract ………………………………………………………………………………………..iv

Introduction ……………………………………………………………………...…………..1

Methodology ………………………………………………………………...…………...2

Current Technology and Near Term Innovations ……………………………..……………… 3

Notional Facial Recognition System ……………………………………………………...8

Long-Term Research and Advancement …………………………………………………...12

Future Applications …………………………………………………………………….. 17

Application One: Intelligence Source Verification …………………………………….. 17

Application Two: Crowd Scanning …………………………………………………… 19

Application Three: Sector Control …………………………………………………….. 20

Roadmap …………………………………………………………………………………….. 21

Conclusion ……………………………………………………………………………… 24

Bibliography …………………………………………………………………………… 26

## Abstract

Facial recognition technology will create the capability to provide positive identification of persons in a battlefield environment in the year 2035. This paper examines the state-of-the-art in facial recognition technology in the areas of access control and law enforcement. The technologies are then projected forward to examine a notional facial recognition system in the year 2035 and examine its components. In discussions with biometric experts from both the United States and United Kingdom, the viability of such a system is examined. Challenges, both in the technology and political/bureaucratic realms, are examined and possible solutions are posited.

The paper poses three scenarios in which a facial recognition system could be of use to Coalition forces operating in a counterinsurgency environment. These three scenarios--passive identification in a crowd, intelligence source verification, and sector control--show the range of applications for facial recognition on the battlefield.

The paper concludes with a roadmap to assist in the focusing of research and allocation of resources as facial recognition technology evolves. With appropriate levels of effort, a technology that is currently capable only in very controlled conditions will evolve into a viable system for positive identification on the battlefield by the year 2035.

# INTRODUCTION

Positive identification of persons in a wartime environment is key to the prosecution of US objectives. On the future battlefield, facial recognition technology will provide personnel the ability to positively identify a person based solely on facial features. Autonomous, remote camera systems placed in high trafficked areas or mounted on mobile platforms will passively scan crowds and identify persons of interest. Friendly forces will be able to cross-reference an individual providing intelligence against previous statements that the individual has made, producing a track record that will be used to estimate the reliability and veracity of any information provided. Sectors of a city or town will be watched and systems will learn about the people who live in that area. If anyone who doesn’t normally frequent the area enters, the system will alert the operators to take appropriate action.

Today, facial recognition technology is still in its infancy. It works very well under tightly controlled conditions. However, as soon as those conditions start to degrade--the face is captured only from the side, is in low light, is wearing glasses, has aged, or even has a different facial expression--the probability of verification drops significantly. For this reason, current applications are primarily in the area of access control and law enforcement since those applications grant the most control over the environment and individual. If any aspect of the environment is out of a certain range, the operator can adjust the camera or the subject.

Several projects in the near term are examining how the verification rate can be increased without requiring complete control of the environment or the subjects. These projects are the building blocks that will enable future systems to autonomously select, identify and process facial data in an unconstrained environment.

## METHODOLOGY

To determine what a battlefield facial recognition system will be capable of in 2035 and determine how to develop tactics, techniques and procedures, this author conducted a series of targeted expert interviews. Biometric team leads from the Pinellas County Sheriff's office, Captain Jim Main and Scott McCallum, provided information on the facial recognition capabilities currently in use in law enforcement. Chris Ferrell of the Concepts and Technologies Branch of the United States Department of Defense (DoD) Biometrics Identity Management Agency, formerly the DoD Biometrics Task Force provided information on multiple projects that the DoD is working on in the five to ten year range. Finally, senior biometric experts in both the United States and United Kingdom were interviewed to determine where the technologies would be moving in the next 25 years and what obstacles might need to be surmounted. Interfacing with organizations in both the US and the UK provided the author with a range of insights into not only technology, but more interestingly on the application of facial recognition. The United Kingdom views the use of video surveillance and license plate recognition with less skepticism than the United States and, therefore, has been using facial recognition technology in law enforcement for some time. The US law enforcement community, on the other hand, tends to eschew many applications of this technology due to Americans' inherent distrust for surveillance systems. While this research focuses solely on the application of facial recognition technology in a wartime environment, where privacy concerns are lessened or non-existent, this divergence in views will most probably lead to differing procedures in the use of such systems.

Based on initial research and interviews, a relevance tree for a notional facial recognition system was constructed to better focus the questioning of the experts, and to facilitate the analysis of the entire system. As interviews and research progressed, the relationship tree was modified to include linkages between key systems. The tree was then analyzed to determine the technologies that need further development in order to achieve the end state envisioned by the experts.

Literary sources were primarily from law enforcement and technical journals. The law enforcement sources provide requirements and insights into tactics, techniques and procedures. The technical journals provided insight into the advances in facial recognition processing that will enable the system. These articles are highly technical and the mathematics is far beyond the scope of this paper. However, they serve to illustrate new directions in the study of facial recognition algorithms as well as future capabilities.

The analysis provides a solid roadmap for the application of an advanced facial recognition system on the battlefield. The paper incorporates three scenarios, indicating the practical application of facial recognition technology.  Specifically, these scenarios address the ability of a facial recognition system to be used for passive identification from a crowd, source verification, and sector control. Both the technological aspects of facial recognition and the development of policies guiding its use are examined, beginning with today's capabilities and culminating in an advanced facial recognition system to be used in 2035.

## CURRENT TECHNOLOGY AND NEAR-TERM INNOVATIONS

Today's facial recognition systems are utilized primarily for law enforcement purposes and to provide access control. Both uses rely heavily on acquiring an image of a person from a specific angle under specific lighting conditions. These requirements are acceptable for a situation in which the operator has full control over the environment. Pinellas County, Florida has one of the leading local law enforcement facial recognition programs in the United States. It uses the facial recognition system at three points in the processing of inmates and also as a means for acquiring information on individuals who have been stopped by police for other infractions and do not possess identification. The system consists of a single still camera that authorities use to acquire a headshot of the subject. In the case of the mobile system, this image is uploaded to a laptop in the patrol vehicle and is automatically sent back to central processing point to match against the existing database.[1] The system returns the top eighty matches to the remote unit for the officer to confirm in the field. The system has two points at which human intervention is required: at the very start of the process in acquisition of the image, and at the very end to make a final match. The core of the process, however is completely automated. As the primary use for this system is to manually determine the identification of an individual who has been stopped for another reason, such as a traffic infraction, the initial human intervention does not detract from the capability of the system--automation is simply not necessary. The system operates in such a manner that in 96% of the cases, the detained individual is included in the first twenty-five returned images.[2] The Pinellas County Sheriff's Department has intentionally placed this final human check into their system and presented the officer with a variety of images so that a human is in the loop for confirmation in the field.

The Sheriff's Department's other application involves the booking and release of inmates. This scenario also uses a system with human interaction at the image capture and final identification. At the pre-booking stage, before the inmate is processed to enter the prison, an image is taken by a trained officer in order to achieve the correct lighting angle and image size, as in the mobile system. Within several seconds his or her entire incarceration history is retrieved and presented to the officer. This data serves not only to verify that the correct individual is being processed, but also provides authorities with medical information in the case of emergencies and his or her criminal history if the inmate is a repeat offender. In the formal booking process demographic data and documentation of any scars or tattoos, along with any other pertinent information is collected by an officer and verified or updated in the database. This provides one final check that the individual is the one that is to be incarcerated and ensures that the prison has the most up-to-date information on that individual. At the end of incarceration, during the release process, the system again verifies that the individual to be released is the one actually released. Similar facilities release the wrong individual once or twice each year.[3] Pinellas County has not done so since the system was put into effect.[4]

The second primary use of facial recognition systems is access control. Similar to the uses described above, access control systems require a specific set of conditions be met in order for the system to function properly. However, unlike the above system, often little or no human intervention is required. As an example, one of the pioneers in the biometric field, Britain-based Aurora, has developed and produced facial recognition access control systems for the construction sector. Due to the nature of construction sites, for safety and security reasons, it is in the construction company's best interest to ensure that only authorized personnel enter. Additionally, logging the authorized individuals at a job site is important to the company's financial bottom line, and can significantly decrease incidences of fraud.[5] Aurora's system has individuals pass through a small turnstile where their faces are imaged. The process automatically detects a human face, selects it, matches it to a database of authorized entrants, and opens the gate. The entire process, from image to access, takes 1.5 seconds.[6] The system was successfully deployed as part of Heathrow Airport's recent Terminal 5 construction effort. During the six-year project, the system successfully allowed access to hundreds of workers each day and "proved an excellent way of enforcing security and reducing fraud."[7]

Present facial recognition systems, like those employed by Aurora and the Pinellas County Sheriff's Department, use certain measurements such as the distance between eyes, the length of the nose, or the shape of the ears.[8] However, these systems have a large degree of control over the image input into the processing system. The face is taken from the same angle, with the same lighting conditions and at a resolution that the system has been optimized for. In a less constrained environment, such as a crowd of people, significant problems arise. "[T]rying to identify individuals in different environmental settings…such as changes in lighting and/or changes in the physical facial features of people, such as new scars[9]" causes modern facial recognition systems to produce inaccurate matches. Systems in development are focusing on ways to identify a single face under "varying facial expressions, viewing perspectives, three dimensional pose, individual appearance, lighting, and occluding structures (e.g. wearing spectacles, facial hair, etc).[10] The solutions currently under development are primarily focused on either compositing multiple images together to produce a more complete image or by creating a new algorithm to better deal with these problems. These pursuits are examined in more detail below.

The Aurora and Pinellas County Sheriff systems serve as examples of the state-of-the-art in facial recognition technology. The Department of Defense Biometrics Identity Management Agency "leads Department of Defense activities to program, integrate, and synchronize biometric technologies."[11] Therefore, they are working on a number of near-term systems across the entire range of biometric technologies. One of their projects which focuses on facial recognition is *Distance Facial Recognition System*.

As noted above, current facial recognition systems are extremely reliable under controlled conditions, but their capability degrades very quickly as the environment becomes less controlled. The Distance Facial Recognition System is attempting to overcome some of those constraints. It began as the Biometric Inmate Tracking System (BITS) developed for the Navy Consolidated Brig in Charleston, South Carolina. BITS was envisioned as an autonomous inmate tracking system for use inside a prison environment in 2002. The system was designed to correlate prisoners' actual location, based on biometric data gathered at control points between zones, with where they were supposed to be. If the inmates' locations did not match, the guards would be alerted. Initially, facial recognition was dismissed as a method of tracking prisoners in favor of fingerprint and hand geometry. While faster and less intrusive "facial recognition produced too many false positives.[12]" However, a follow-on project did incorporate facial recognition as a method of identifying and tracking inmates.

The Facial Recognition at a Distance project began in April of 2008 and continued with the same premise:  tracking inmates inside a prison. The system is a real-time surveillance system that acquires facial images from a distance. It uses two cameras:  a wide-angle master video camera which maintains a set field of view; and a second slave camera that can pan, tilt, and zoom. The master camera views the entire surveillance area and the video is used to detect any human faces in its field of view, without actually identifying them. The system also uses this video to estimate the faces' speed, direction, and orientation, in order to predict the best time and location for targeting. Each face in the field of view is prioritized for identification. The face that is the easiest to identify, based on a variety of factors such as speed, angle, and distance, is then targeted by a second camera.

The second camera, called the slave, then tracks and zooms in on the selected face in order to acquire a high-quality image. This image is processed though an existing facial recognition system in order to recognize the individual. This match is made against a database of the facility's 300 inmates in near real time.[13] Once a match has been made, the process is repeated for each face detected in the master camera's field of view. In the study, which is scheduled to be completed in the spring of 2010, the facial recognition system will be tested with inmates at various ranges up to 60 feet away from the camera. Inmate motion will also be varied from directly toward the camera to perpendicular to the field of view at various speeds. The critical component the project intends to improve upon is the control of the slave camera and the analytical software that captures multiple frames of video and composites them into an appropriately high-resolution image that can be processed by the facial recognition software.

The next phase of the project, just started in February 2010, will focus on enhancing the facial detection algorithm on the master camera video feed to "accommodate wider variations of illumination and shadows on the face.[14]" The system will also examine a new capability: if the system encounters an unidentified face, the system operator would be presented with the images and informed that no match was found. The operator would then be given the option to manually identify the individual and to add those images to the database so that the system would be able to recognize the individual again in the future. While this component would serve little practical use in the controlled environment of a prison, where every individual would be enrolled in the system, the ability to identify new faces and ad them to the database is a technology that will be of much use, as will be described below.

## NOTIONAL FACIAL RECONGITION SYSTEM

A facial recognition system can be broken down into three primary components: capture, processing and dissemination. The entire architecture is presented in Figure 1 below for further clarification. The capture component consists of a camera or cameras which take some image of the environment. In some cases, the capture component simply provides a series of images independent of any input from the rest of the system, such as a single video camera trained on a chokepoint. More often, though, the camera is controlled by either an operator or some feedback loop from the processing component. In a dual camera video system, the operator or processor would detect faces from the wide-angle image and feed them back to the pan-tilt-zoom camera to zoom in and acquire an image. Present systems, such as the Pinellas County Sheriff's Department booking system, are fully dependent on an operator acquiring a facial image that is then presented to the processor.

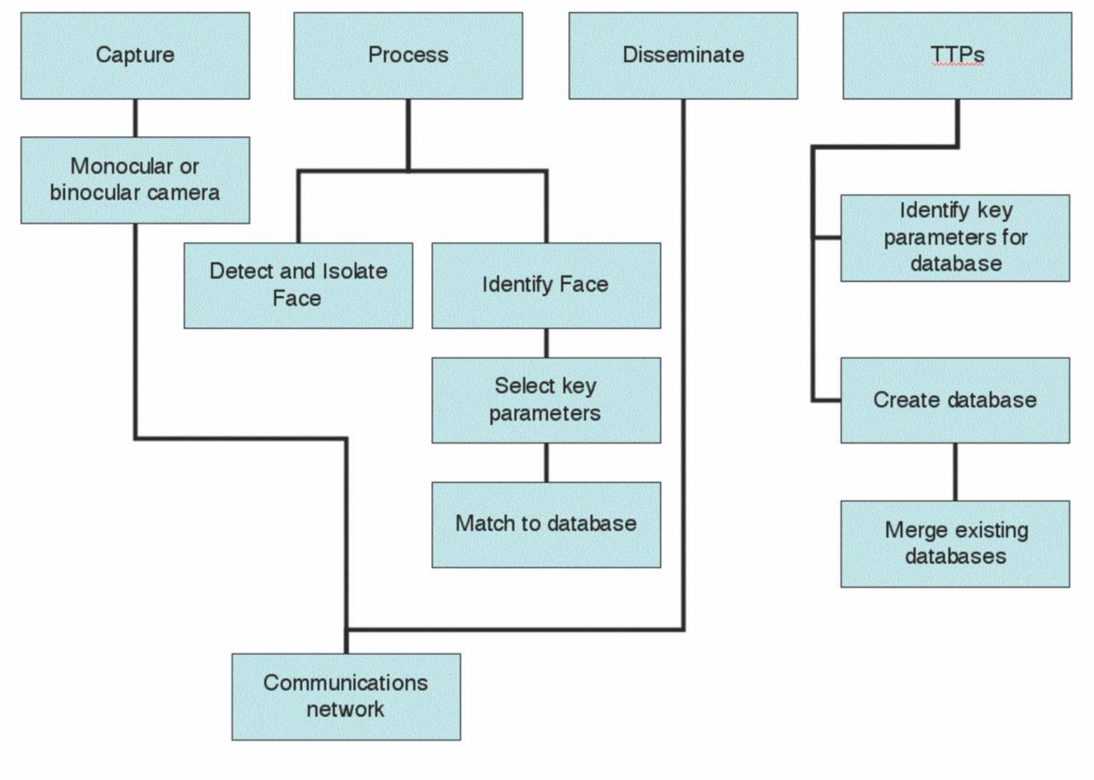

Figure 1. Notional Facial Recognition System.

In the future, these systems will retain their function, but capture and isolate faces from a much larger stream of data. High resolution video systems, such as those described below will be able to capture orders of magnitude more data in one video frame than today's mid-range consumer digital camera.[15] The capture systems will be fully antonymous, with no need for an operator to identify a face and ensure that it is at the proper angle. Multiple cameras will be able to track an individual as he moves across a street or into another room. The networked sensors will be able to reacquire him and continue to capture images from multiple angles[16]. These images will then be pre-processed and the templates will be passed along to the processing component.

The processing component is the core of the facial recognition system. Its two primary subsystems are the facial detection system and the facial identification system. The facial detection system analyzes the images presented to it and isolates facial images. These images are then provided back to either the capture system, to provide a higher resolution image with the pan-tilt-zoom camera, or to the facial identification system in order to actually match the face. Once the facial image is provided, the image is broken down into components, depending on the algorithm used to perform the facial matching. For example, the system determines the distance between the eyes, the length of the nose, and other required parameters. It then creates a template, or a set of data that represents the parameters measured. This template is compared to a database which contains the templates of multiple faces. The faces whose templates most closely correlate to the target image are then provided to the dissemination system. In the case that no templates match with certainty, that result would be provided to the dissemination system.

A future facial recognition processor will differ from its modern counterpart in a number of fundamental areas. Receiving data from the capture component the system would identify faces not in single frames, but detecting them across video. These multiple images would be composited together to create a higher resolution or a three-dimensional image. The core of the system, the matching algorithm will change. Modern matching algorithms are reaching their limit with the amount of faces in the databases.[17] These new algorithms will be optimized for specific conditions. If the processor receives a low-resolution image, it will be run through one algorithm; if the image is an oblique angle, it is run through another algorithm; if the image is dark, another. Allowing images to be run through the most efficient algorithm for that particular image will decrease the matching time and increase accuracy. Different algorithms could also be used based on different ethnicities. Certain algorithms tend to perform well within the ethnicity of the developers, based upon how it is trained.[18] Any single image could be analyzed by multiple algorithms based on the content and quality of the image. Since the system would be working in near real time, if the matching algorithms did not return any matches, the processing system could request that the capture system reacquire an image of the subject's face. Or, if the processor deemed that the image was of high enough quality, but no match existed in the database, it could enroll that face and begin to build a profile around it.

The dissemination component is the least complicated of the systems. It takes whatever results are presented by the processing system and provides them to the appropriate entity. The component can provide as little or as much data as is called for, depending on the facial recognition system's function. In the case of an access control system, the component would simply allow the individual access and log the entry. In the mobile system in use by Pinellas County the system returns the top 80 matches, in order of certainty, to the officer in the field, so that a human can make the final determination.

In the future, as in the present, this dissemination system will be tailored to the system it is designed to support. The speed of the network will be faster and allow greater data throughput. The system will be largely antonymous, providing information to the operator only when needed to be acted upon. In many cases the system will disseminate the information to another component of the facial recognition system, instead of to an operator, such as the case of enrolling a new face in the database.

The fourth aspect of the facial recognition system is not actually a technology component, but the tactics, techniques and procedures that guide the use of the system and the collection of the databases. Today the databases used are spread throughout the US Government and beyond. The Department of Homeland Security maintains or has access to at least five distinct biometric databases for multiple purposes. It has access to the FBI's terrorist watchlist, which contains approximately 1.7 million persons. It maintains a list of persons who have applied for visas consisting of over forty million entries. In all, DHS has access to over fifty million entries spread across multiple databases.[19] With that amount of data, and dozens of facial recognition technology projects in progress across the government, it is essential that all efforts be synchronized and for the immense data collection component to be compatible across all systems.

## LONG-TERM RESEARCH AND ADVANCEMENT:

In the author's interviews with senior biometrics experts within the governments of the United States and the United Kingdom, the individuals were asked to postulate where technology would be in 25 years. Departing from the current system of using a combination of wide angle camera and pan-tilt-zoom camera to detect and then identify faces in a large space, the UK biometric expert felt that the current interest in scanning cameras that produce a single gigapixel image indicate the directions the technology is moving. In 2009 researchers in the Netherlands used a computer-controlled camera to take and stitch together 600 images of the city of Delft.[20] The resulting 2.5 gigapixel image provides a clear view of an entire cityscape, completely zoomable down to individual people in certain areas. While not taken in one shot, the ever-increasing resolution of consumer and professional digital cameras serves to indicate that the resolution of off-the-shelf video cameras will increase over time. Current HD video cameras can shoot at a resolution of 1920 x 1080, or approximately 2 megapixels. The Japanese Broadcasting Corporation is investigating a system that would record at over 33 megapixels.[21] At that resolution, a face that occupied less than 1% of the entire frame could be detected and identified with present technology.

Further discussion on this concept with the UK expert examined what communication network would be required to support such a system. Due to the immense amount inherent in such a high-resolution video stream, it would overload the network if the raw video was transmitted to a central processing facility in order to run facial recognition algorithms upon it. Required network traffic could be substantially decreased by filtering the image at the collection point. Each frame would be compared to the previous frame for motion, and those areas of the frame that did not exhibit motion would be discarded. The remaining images would be further analyzed with a simple facial detection algorithm. Those areas of the frame that don't contain faces would be discarded. At this point, depending on the situation, it might be possible to send the facial images back to the processing facility. However, if the camera was in a highly trafficked area, it might not be practical to send that amount of data across the network. In this case, with the addition of a small amount of computing power, roughly equivalent to a modern notebook computer,[22] the image could be broken down into a template to be matched. This would reduce the amount of data transmitted by 90%.[23] In the end, a facial template of less than a kilobyte would be sent back from the original image--which could be as large as 200 megabytes for a 33 megapixel camera.

The data collected by such a camera could be put to further use as well. The UK expert believes that as the camera captures full-motion video, the on board processing system could also use sequential frames to composite a face. If a subject walked into frame, showing only a profile to the camera, the image would not be as useful as a frontal image. Yet, if the subject turned his head as he was walking, each frame would be captured and composited together to create a more complete image of the face. A further advantage to this process is that the image would be able to be constructed in three dimensions. This facial map would be able to be broken down into a template in the same manner as the two-dimensional image, but it would able to be run through a more rigorous algorithm, enhancing the ability to positively match the subject.

If the individual remained still, the camera could catch multiple images of the same pose. Another process, image stacking, could combine these images, picking out details from each of them and produce a virtual higher resolution image. This virtual image could then compensate for a lower resolution image captured on the original feed, or it could be used as another biometric modality, such as skin texture, to provide a greater confidence in the match. The team of experts from the United States indicated that the law enforcement community in the United States is very interested in three-dimensional facial recognition, but the concept is not heavily funded within the federal government. Three dimensional technology today consists mainly of manipulating a still image that provides an oblique angle face and correcting the perspective so that the visible portion of the face is in the correct proportion to be analyzed by a traditional frontal facial recognition program. Three-dimensional facial construction is the other side of the same coin. Hollywood has been investing heavily in better and better modeling systems to produce movies such as *Avatar*. The government could leverage that technology base to begin to explore the application of three-dimensional facial recognition technologies. Unfortunately, organizations are focusing on near-term solutions that can produce results in three to five years, such as tweaking existing algorithms, but there is no concerted effort to examine what the next generation of facial matching algorithm will be.

In discussing the technologies needed to develop the viability of facial recognition technology, the UK expert asserted that while raw computing power would provide some boost in performance, as would distributed computing, in the end the number of faces in any database would begin to cause existing algorithms to return too many false positives. Essentially, what is required is not more or faster computer power, but better algorithms that can deal with both a large database and a facial image that may not be ideal.

A new approach to facial recognition was introduced in late 2009 by a team from the University of Illinois at Urbana-Champaign. Led by Dr Yi Ma, the team has developed a novel approach to matching faces. Instead of measuring features, which account for a very small percentage of the actual face, it compares randomly selected pixels from the facial image and compares those pixels against the database. While the mathematics behind this method are beyond the scope of the paper, the author of the algorithm provides this analogy:

> Assume that a normal individual, Tom, is very good at identifying different types of fruit juice such as orange juice, apple juice, lemon juice, and grape juice. Now he is asked to identify the ingredients of a fruit punch, which contains an unknown mixture of drinks. Tom discovers that when the ingredients of the punch are highly concentrated on a single type of juice (e.g., 95% orange juice), he will have no difficulty in identifying the dominant ingredient. On the other hand, when the punch is a largely even mixture of multiple drinks (e.g., 33% orange, 33% apple, and 33% grape), he has the most difficulty in identifying the individual

> ingredients. In this example, a fruit punch drink can be represented as a sum of the amounts of individual fruit drinks. We say such representation is *sparse* if the majority of the juice comes from a single fruit type. Conversely, we say the representation is not sparse. Clearly in this example, sparse representation leads to easier and more accurate recognition than nonsparse representation.[24]

Thus, Ma has created an algorithm to exploit this sparse representation. The algorithm provides much more accurate results than traditional facial matching algorithms. In studies under a variety of lighting conditions, the sparse representation algorithm correctly matched 96% of faces without glasses in a generally frontal view.[25] As would be expected, the performance did decrease as less control of the subjects was exercised. The study examined subjects who were wearing eyeglasses and sunglasses, making noticeable expressions, out of focus, and with motion blur. In the most extreme cases, recognition dropped to just over 50%.[26] However, one significant advance of the algorithm is the ability to cope with the very common problem of occlusion, the covering of certain parts of the face. Ma's "algorithm can handle up to 80% random corruption of the face image and still reliably recognize a person."[27] This is an exceptional performance increase over traditional facial recognition systems, in which accuracy "declines to less than 70% when part of the face is covered." This new algorithm may be the next step in facial recognition technology and should be examined further by the United States Government. It "is scalable both in terms of computational complexity and recognition performance. … [It] is directly compatible with off-the-shelf face detectors and achieves extremely stable performance under a wide range of illumination, misalignment, pose and occlusion."[28] The fact that it is compatible with existing technologies and is scalable is crucial, since any new facial recognition system must access legacy technology and work with an ever-growing facial database.

With the improvement in algorithms, though, comes the requisite re-enrollment of the entire database. The State Department recently upgraded their algorithm for their visa matching program. The conversion process took six months to update the 41 million entries in the database to work with the new algorithm. The upside is that it was possible. Facial recognition's core dataset is a visual representation of the face. This raw data is archived after it is processed to create new templates as algorithms change. This must process must be continued as new databases are created. Biometrics in general, and facial recognition in particular, are evolving fields and as algorithms change there must be a way to keep the collected data relevant in light of the new algorithm.

## FUTURE APPLICATIONS

Having examined the technical aspects of long-term study, three scenarios are presented below, both in the context of the present and the future. These scenarios incorporate the advances noted above and demonstrate the application of a future facial recognition system in a future battlefield environment.

## APPLICATION ONE: INTELLIGENCE SOURCE VERIFICATION

*At an outpost on the outskirts of a town a local national approaches a guard. He claims to have information relating to an attack planned against a US facility. The individual is searched and escorted to meet with an agent who receives the information. Seemingly credible, and with no information to contradict what the source has offered, the information is passed along and resources are diverted to enhance the protection of the facility. Time passes but the attack doesn't materialize. A week later the same individual (although unknown to Coalition* *forces) appears in another city and provides a similar false story. This time he has altered his appearance by trimming his hair and wearing eyeglasses. His headgear now covers the scar across his forehead. He provides a different name to the agents. Again, resources are diverted and again, no attack is made. After confirming that force protection will be altered, and in what specific manner, the individual provides false information at another location, but this time an attack is launched at a location that has become more vulnerable due to reinforcements provided to protect the other facility. Force protection assets responding to the location of the supposed attack are themselves attacked executed by terrorists based on the observed practices form the initial false reporting.*

The reliance on human intelligence in today's wars is immense. Tracking the reliability (or lack thereof) of a human source of information in 2035 would be significantly enhanced through the use of an advanced facial recognition program providing near real time information in a changing environment. The current process of requiring a source to submit to some form of active biometric, such as taking a fingerprint or imaging a retina lets the source know s/he is being tracked, which can discourage some sources from providing any information at all.

A passive facial recognition system, collecting sources' faces without their active participation, would be able to catalog and connect him with the entirety of information he has provided, regardless of where or to whom that information was provided and add a level of verification and warning not currently available. The individual providing false and misleading information in this scenario would have a greater chance of being associated with false past reporting, a greater chance of his information being more thoroughly vetted, and stand a greater chance of being detained and questioned as to the motives of earlier false reports. In essence, he will be countered using facial recognition technology. Specifically, upon his initial approach of the facility he would be imaged and matched against known informants and tagged as a new informant with no history of credibility. When the attack doesn't materialize, a flag would be placed in the database indicating this. During his second approach he would be identified by the facial recognition system despite the alteration of his features. He might still give a false name, and the discrepancy of the two names he provided would prompt authorities to probe further and possibly apprehend a double agent with nefarious intentions, or even prevent a future attack based on those intentions.

## APPLICATION TWO: CROWD SCANNING

*Without specific targeting information, random chance plays a large role in discovering persons of interest. Sitting below the High Value Target threshold, these people can easily blend into local populations. Consider a small team operating in a counterinsurgency environment. The team moves through a densely populated area. They pass through crowds of tens or hundreds of people, most of a different culture and racial heritage. An overriding concern to the team is personal safety--both their own and their fellow team members. That sector of the city has played host to more than a few firefights, and the team is understandably focused on threats which occupy a large part of their situational awareness. In their briefing that morning they were shown mug shots of a dozen different individuals suspected to be located in that sector who are wanted for questioning. As the team picks its way through the congested streets, a member notices a face that seems familiar. He alerts the team and they move towards the individual, maintaining situational awareness of the security threat around them, but no longer searching the environment at large for a suspected target. They approach and apprehend the targeted individual, but he isn't on their list—he simply looks similar. In the meantime, however, an* *individual who is wanted and known to Coalition forces, but wasn't on the list highlighted that morning, slips past the team.*

Twenty-five years in the future, the same team moving through the crowds would be equipped with video cameras attached to their helmets or vests. These cameras would be wirelessly linked to a processing system miles away. As the camera autonomously scans the crowd each individual in the crowd is imaged and instantly matched against a database of persons of interest. It alights on one individual and alerts the team. As the team approaches, the system continues to image the target to confirm that it is the person of interest, indicating a percentage match to the team members' integrated heads-up-displays. While doing this the team's cameras continue to scan the crowd, searching for additional persons of interest. The team's energies, meanwhile, are focused on approaching the individual safely and questioning him. Additional scanning and the use of complimentary advanced identification means confirms the target is a person of interest and he is subsequently apprehended, maximizing the chances of a safe outcome for the team, the target, and the surrounding civilian population.

## APPLICATION THREE: SECTOR CONTROL

*In one neighborhood that has a relatively low level of violence a stranger appears. He watches the way people and traffic move. He watches American forces maneuver through the neighborhood. He blends into the local population--after all, he lives just across the city. Only those who have lived on that street all their life notice him, and even they don't give him a second thought. Ten days after his first appearance, an IED explodes as American forces pass by. Several vehicles are destroyed, four Americans and 13 local nationals are killed. Dozens more are wounded.*

In the future, passive video systems will be able to record each individual in a city and provide a history of his location. This is an advanced "human" approach to systems already in use in the United Kingdom. That system passively tracks license plates as vehicles pass certain checkpoints. The data is primarily used to charge fees for entering certain high congestion zones in and around London, but has also been used to track stolen vehicles or vehicles linked to criminals wanted for questioning.[29] If an individual who spent a preponderance of his time in one area suddenly and consistently appears in another area, it would raise concern. There are many legitimate reasons that his travel patterns have changed, such as a new home or new friends, but an advanced facial recognition system would provide one more tool to allow for further investigation if something is a little out of place—which is often all that is needed to prevent an attack.

## ROADMAP

The human brain is simply not equipped to identify a single, relatively unfamiliar face from among the hundreds in a large crowd. On the modern battlefield, identifying a person requires a very specific chain of events to occur, starting with remembering a specific face and culminating with making the visual connection in a crowded and stressful environment. Advanced facial recognition technology could passively sweep a large crowd of people very quickly. This data, with the aid of new software and hardware, would be matched with a set of linked facial recognition databases. The matches would provide the individual on the ground with near-real-time information relating to specific persons of interest in his or her vicinity.

Based on research performed as part of this project, the largest technical challenge in making a future facial recognition system a reality comes from the core of a facial recognition system, the hardware and software that actually correlate the data sets. With current technology, facial images have to be taken from certain angles or be under certain lighting conditions in order to allow the software to operate correctly. Four states now prohibit individuals from smiling in driver's license photos as the expression degrades the ability to match the photo with an existing one in the state's inventory, enabling a person to obtaining two separate ID's.[30] The application of new software algorithms, such as sparse recognition noted earlier, will allow facial recognition systems to surpass these technological limitations. Software that combines multiple views of the same face, whether compositing multiple angles together into a three-dimensional image or stacking similar angles on top of each other to produce a virtual high resolution image, will enable higher quality models. These models can then be run through algorithms that are tailored to the set of data that has been acquired. Current capabilities enable facial recognition from video sources, but can only detect a small number of faces within the frame and only match it against several hundred images before becoming overwhelmed. The exponential growth of computing power, specifically integrated circuitry and molecular computing, Ray Kurzweil's the sixth paradigm, will allow for vastly improved performance in processing capability over the next twenty-five years.[31] However, none of the experts the author interviewed believed that the simple application of more computer power could solve the processing problem of a large facial recognition system. They did agree that the development of a new algorithm specifically designed for such a purpose would be the most beneficial advance to facilitate matching facial images in real-time and against a large database.

The processing component will be the core of any future facial recognition system. However, the ability to identify an individual in a crowd will require a collection source. This collector, most probably a video camera or similar device, will require a high capacity path to the processor. In order to optimize the balance between processing and network saturation, it is important that a fair share of pre-processing be done at the point of collection. This pre processing, ranging from simply isolating the facial image to generating a facial template, significantly decreases network utilization. This architecture would still require a high-capacity data transfer conduit from the collector to the processor. With bandwidth at a premium in a wartime environment, compression would be imperative. Such an architecture would also open the system to jamming, though the system would be no more or less vulnerable that any other fielded communication system.

The need for a common database or, at the very least, multiple linked databases is perhaps the most difficult obstacle to be overcome as the problem is not based in technology, but in the requirements, budgets, and politics of many different organizations across the United States Government. For years, multiple organizations have kept some sort of facial recognition data. Its most basic form, the mug shot, has been in use since the 19th century. The United States has well over 50 million facial templates spread across multiple databases. That number is growing at a rate of over six million entries each year in visas alone.[32] Technologically linking databases would be relatively easy. The significant problem will be to come to a consensus on exactly what data should be contained in that database. Once the data set is determined, it would be technologically insignificant to link multiple databases. However, the different entities that would maintain individual databases (AFOSI, NCIS, CIA, FBI, EUROPOL, INTERPOL, etc.) would need adequate assurance that proprietary or classified data within an individual database would remain unviewed and untouched in the linking process. While this is a minor technological issue when compared with those described below, it is not an insignificant one and must be addressed.

## CONCLUSION

Due to technological limitations, facial recognition technology is presently only used in environments that can be tightly controlled. However, the technology has the potential to be a critical component on the battlefield in twenty-five years. Advances in optics and video systems will enable the collection of large amounts of video data. Advances in computer technology will enable the detection of multiple faces from full motion video. Image processing software and three-dimensional facial imaging technology will lead to the ability to build three-dimensional models based on two-dimensional video streams and create higher resolution still frame images through image stacking. The development of new facial recognition algorithms will allow faces plucked from these collection sources to be matched against databases filled with of hundreds of millions of templates. The fusion of databases will allow the systems to interconnect and match faces against these templates, regardless of what organization collected the data or now maintains it.

The technological aspects are solid. While advances are still being made, experts on both sides of the Atlantic feel that the notional system described above is very possible within the twenty-five year horizon examined in this paper. The biggest roadblock they can envision is the political aspect--whether or not disparate organizations can work together to develop an interoperable standard for their facial recognition databases. If this obstacle is to be overcome, the United States Government as a whole needs to prioritize the development of interoperable facial recognition systems. Due to the inherent data ownership and classification concerns, such as intelligence agencies accessing law enforcement records, separate databases would still need to be maintained. Likewise, depending on their function, facial recognition systems would necessarily perform different actions, as they should be in order to maximize their performance. These two components, the facial recognition systems themselves and the databases behind them, are expected to be tailored to the activities they support, But the systems should be built modularly and interoperability so that, providing all applicable legalities are met,  any database can accessed by any facial recognition system. If this fundamental design tenet is followed, a robust facial recognition system that will function in an unconstrained battlefield environment is completely plausible by the year 2035.

[1] *Facial Recognition for Law Enforcement*, Pinellas County Sheriff's Office, 2009.

[2] Jim Main (Pinellas County Sheriff's Department) interview with the author 10 March 2010.

[3] *Facial Recognition for Law Enforcement*, Pinellas County Sheriff's Office, 2009.

[4] Ibid.

[5] Lee Hibbert, "Face to face," *Professional Engineering* 22 no. 5 (11 March 2005): 23.

[6] Ibid.

[7] Ibid.

[8] Jim Main and Scott McCallum (Pinellas County Sheriff's Department) interview with the author 1 April 2010.

[9] Ravi Das, "An introduction to biometrics," *Military Technology* 29 no. 7 (July 2005): 23.

[10] Raymond S. T. Lee, "iJADE Authenticator — An Intelligent Multiagent Based Facial Authentication System." *International Journal of Pattern Recognition & Artificial Intelligence* 16, no. 4 (June 2002): 482.

[11] Department of Defense Biometrics Identity Management Agency Web Site, "*Mission-Vision*," http://www.biometrics.dod.mil/About/mission.aspx

[12] Christopher A. Miles and Jeffrey P. Cohen, "Tracking Prisoners in Jail with Biometrics: An Experiment in a Navy Brig," *NIJ Journal*, no. 253 (January 2006), http://www.ojp.usdoj.gov/nij/journals/253/tracking.html

[13] Chris Ferrell (Concepts and Technology Branch, Biometrics Identity Management Agency) interview with the author 10 February 2010.

[14] Presentation by the Biometrics Identity Management Agency to the FBI, "*Facial Recognition Projects*," 29 January 2010.

[15] M. Kanazawa et al, "Ultrahigh-Definition Video System with 4000 Scanning Lines" *International Broadcasting Convention Publication*, (2003), 321.

[16] Interview with senior United Kingdom biometrics expert, 31 March 2010.

[17] Ibid.

[18] Jim Main and Scott McCallum (Pinellas County Sheriff's Department) interview with the author 1 April 2010.

[19] Presentation by the Department of Homeland Security, "*DHS Multi-Biometric Fusion Research Plan*," 2010.

[20] "The (Really) Big Picture." *Communications of the ACM* 48, no. 2 (February 2005): 10.

[21] M. Kanazawa et al, "Ultrahigh-Definition Video System with 4000 Scanning Lines" *International Broadcasting Convention Publication*, (2003), 321.

[22] Jim Main and Scott McCallum (Pinellas County Sheriff's Department) interview with the author 1 April 2010.

[23] Ibid.

[24] Allen Y. Yang, "Robust Face Recognition via Sparse Representation -- A Q&A about the recent advances in face recognition and how to protect your facial identity," http://watt.csl.illinois.edu/~perceive/recognition/Files/YangA_FaceRecognitionQandA.pdf

[25] Andrew Wagner et al, "Towards a Practical Face Recognition System: Robust Registration and Illumination via Sparse Representation," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2009: 8.

[26] Ibid.

[27] Kirk L. Kroeker, "Face recognition breakthrough" *Communications of the ACM* 52 no. 8 (August 2009): 19.

[28] Andrew Wagner et al, "Towards a Practical Face Recognition System: Robust Registration and Illumination via Sparse Representation," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2009: 8.

[29] Christine Evans-Pughe, "Road watch [automatic number plate recognition system]," *Engineering & Technology* 1 no. 4 (2006): 1.

[30] Thomas Frank, "No license to smile at some dmvs". *USA Today*, 26 May 2009.

[31] Ray Kurzweil, *The Singularity is Near* (New York, NY: The Penguin Group, 2005), 67.

[32] United States Department of State, "Summary of Visas Issued by Issuing Office: Fiscal Year 2009," http://www.travel.state.gov/pdf/FY09AnnualReport_TableIV.pdf

## Bibliography

Bowman, M. E. “Law enforcement technology, intelligence and the war on terror,” *Military Technology* 31 no. 10 (November 2007): 127-134.

Biometrics Identity Management Agency Presentation to the FBI, “*Facial Recognition Projects*,” 29 January 2010.

Das, Ravi. “An introduction to biometrics,” *Military Technology* 29 no. 7 (July 2005): 20-27.

Department of Defense Biometrics Identity Management Agency Web Site, “Mission-Vision,” http://www.biometrics.dod.mil/About/mission.aspx

Department of Homeland Security, “*DHS Multi-Biometric Fusion Research Plan*,” 2010.

Evans-Pughe, Christine. “Road watch [automatic number plate recognition system],” *Engineering & Technology* 1 no. 4 (2006): 1.

Ferrell, Chris. (Concepts and Technology Branch, Biometrics Identity Management Agency) interview with the author 10 February 2010.

Frank, Thomas. “No license to smile at some dmvs.” *USA Today*, 26 May 2009.

Hibbert, Lee “Face to face,” *Professional Engineering* 22 no. 5 (11 March 2005): 22-23.

Interview with senior United Kingdom biometrics expert, 31 March 2010 (interview was conducted in confidentiality and the names of interviewees are withheld by mutual agreement).

Interview with senior United States biometrics experts, 31 March 2010 (interview was conducted in confidentiality and the names of interviewee is withheld by mutual agreement).

Kanazawa, M. et al. “Ultrahigh-Definition Video System with 4000 Scanning Lines” International Broadcasting Convention Publication, (2003), 321.

Kroeker, Kirk. “Face recognition breakthrough” *Communications of the ACM* 52 no. 8 (August 2009): 18-19.

Kurzweil, Ray. *The Singularity is Near* (New York, NY: The Penguin Group, 2005), 67.

Lee, Raymond S. T. “iJADE Authenticator — An Intelligent Multiagent Based Facial Authentication System.” *International Journal of Pattern Recognition & Artificial Intelligence* 16, no. 4 (June 2002): 481.

Main, Jim. (Pinellas County Sheriff’s Department interview with the author 10 March 2010 Pinellas County Sheriff’s Office, *Facial Recognition for Law Enforcement*, 2009.

Main, Jim and Scott McCallum. (Pinellas County Sheriff’s Department) interview with the author 1 April 2010.

Miles, Christopher A. and Jeffrey P. Cohen. “Tracking Prisoners in Jail with Biometrics: An Experiment in a Navy Brig,” *NIJ Journal*, no. 253 (January 2006), http://www.ojp.usdoj.gov/nij/journals/253/tracking.html

Park, Sungsoo and Daijin Kim, “Subtle facial expression recognition using motion magnification,” *Pattern Recognition Letters* 30 no. 7 (August 2009): 708–716.

“The (Really) Big Picture,” *Communications of the ACM* 48, no. 2 (February 2005): 10.

United States Department of State, "Summary of Visas Issued by Issuing Office: Fiscal Year 2009," http://www.travel.state.gov/pdf/FY09AnnualReport_TableIV.pdf

Wagner Andrew et al. "Towards a Practical Face Recognition System: Robust Registration and Illumination via Sparse Representation," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* June 2009: 8.

Yang, Allen Y. "Robust Face Recognition via Sparse Representation -- A Q&A about the recent advances in face recognition and how to protect your facial identity," http://watt.csl.illinois.edu/~perceive/recognition/Files/YangA_FaceRecognitionQandA.pdf