Facial Recognition: A Biometric For The Fight Against Check Fraud

Gary S. Reynolds
Wells Fargo Bank

Abstract

While facial recognition technology holds promise for solving many identification/authentication problems, its use has been limited to known populations where individuals are identified, enrolled, and assigned a personal identification number. Because the technology is now more robust, this study examined the feasibility of using it to mitigate over the counter check fraud. It explored the use of facial recognition technology in a novel application, integrating it in into a fraud management program. Facial recognition technology was installed at fifteen bank branches to test its reliability in identifying persons on a watch list and a control group. Three groups were used: fraudsters, bank robbers, and a control group of participants. The results indicate that facial recognition systems have the potential for reducing fraud in these transactions, but several obstacles must be researched and overcome.

Introduction

The crime of fraud continues to become more sophisticated. Frank Abagnale, the subject of the book and movie *Catch Me If You Can,* stated at the Financial Services Information Sharing Analysis Center (FS-ISAC) 2005 Members Conference, “Annual losses from fraud are almost twice the federal defense budget at $660 billion dollars.” Additionally when speaking of identity theft he said, “Identity theft is a simplistic crime where anybody can become anybody.” Abagnale also stated that, “Technology breeds crime” (2005). Assuming that this is true, then new technologies, such as facial recognition should be able to deter and prevent crime.

Currently, in a typical check fraud, the customer notifies the bank of the fraud, either by phone, e-mail, or in person. Between the time of discovery by the customer and reporting to the bank, 30 – 60 days can elapse. This lag time is partially caused by the bank statement cycle which is prepared and sent every 30 days. This reporting delay can impact the investigation as often times the trail is cold with little or no leads.

Once reported, the claim is then researched, and if validated, sent to the investigations department. The investigator receives the information and a new case is opened. He or she will research the transaction and use the transactional information to locate and retrieve a photograph of the fraudster from

the branch bank's Digital Video Recorder (DVR). This process can take hours, because the investigator has to validate that the transactional information matches up to the person who conducted the fraudulent transaction. To further complicate matters, teller terminals and surveillance cameras are moved from time to time because they become damaged or require service. This can cause transactional numbers to appear at the wrong teller station, which in turn causes the investigator to have to search large amounts of video to identify the fraudster. If the fraudster is unknown to the investigator, the investigator may contact law enforcement or peer investigators at other institutions in an attempt to learn the identity or claimed identity of the fraudster. All the while the fraudster may be committing more fraud at other branch banks. The cycle of investigative activity starts over each time the fraudster cashes a forged check and occurs both internally and externally to financial institutions. Presently there is no automated searching of the branch bank DVRs for the fraudster, because facial recognition technology is not used as a fraud detection or prevention tool and is not integrated into the existing DVR system.

In 2004 the American Bankers Association conducted their ABA Deposit Account Fraud Survey. They found that the number one threat against banks was check fraud. Seventy five percent of commercial banks experienced losses from check fraud. These losses were estimated to total $677 million. The leading method of check fraud in the survey was forged maker, i.e. the fraudster who forges the signature of the maker and personally presents the instrument at the bank (Association, 2004).

Why Facial Recognition Technology

There are several biometric technologies that use pattern recognition to verify an individual's claimed identity or identify against a population of known identities. RAND lists eleven different biometric technologies that are either being studied or are already in use (Woodward Jr., Horn, Gatune, & Thomas, 2003). Biometric identifiers are used in many ways, such as to gain access to a secure facility or to validate an individual who conducts some type of financial transaction. Computer assisted biometrics technologies may be mature enough to support a move from verification that asks, "Are you who you say you are?" to identification that asks, "Who are you?" (Norton & Ryan, 2005). The four phases of engaging a biometric system include enrollment, storage, acquisition at time of presentment, and matching. One of the main advantages that biometrics has over other digital identifiers is that the biometric is part of the body so it will always be present, never forgotten, never left at home (Maghiros, Punie, Delaitre, Lignos, Rodriguez, Ulbrich, & Marcelino, 2005).

There are three ways the biometric process can be used. Verification is the process of identifying who you say you are with a one – to – one (1:1) match. Identification is the process used to discover the identity of an unknown person with a one – to – many (1:N) match. Screening is the process that uses a watch

list containing data on individuals to be identified because they may be persons of interest or wanted persons with a one – to – few (1:Few) match (Woodward Jr., Orlans, & Higgins, 2003). This study focuses on the screening processes.

"Humans possess an extraordinary visual system capable of learning and recognizing thousands of faces – even someone they don't know and have never seen" (Tucker, 2003, p. 5). Human recognition differs from computer facial recognition. Humans use a variety of observations when making their recognition decisions. These might include the voice, in some instances a person's gait, perhaps the time of day an individual is expected, and even how someone gestures as they speak. Humans do better when looking for someone they know. Facial recognition systems do equally as well when searching for someone who is unknown. Humans do not do as well when presented with just a static photograph absent other indicators (Roark, O'Toole, & Abdi, 2003). It is difficult to glance at a customer's driver's license and make an instant decision on whether they match. Combine this with the added responsibility of looking at the fraud watch list while conducting normal business transactions and the process becomes very complicated. The problem is the amount of time it would take for enough trained employees to study the list of persons wanted for check fraud so that they would be able to recognize someone on a fraud watch list. While humans might be able to learn the faces and recognize them, computers using facial recognition technology should be able to do as good or a better job.

Facial recognition technology is the one biometric that has wide public acceptance and is considered the least intrusive of all other technologies (Maghiros et al., 2005). Enrollment can be passive: a person entering a business equipped with facial recognition technology is automatically enrolled in the system. If the quality of the photograph is poor, some social engineering may be required to get an image that will work. While fingerprints are widely accepted as a means of identification, at some point there has to be face to face physical or at least machine to finger contact with the person. Scanners that use irises or retinas as a biometric identifier require not only near contact with the scanner to use the system, but enrollment can be an uncomfortable process for the individual. There are also concerns about disease transmission from near contact with the scanning device. Palm print or hand geometry also requires direct contact with the person. The readers require direct contact with the scanning device as well as a personal identification number (PIN) in most cases. The concerns about disease transmission through contact with the scanner are unfounded, as there are certainly more opportunities to touch door knobs and stair railings in a day than palm or hand scanners.

In addition to the enrollment advantages, automated facial recognition systems are constantly being updated as new faces are acquired. It is also very easy to explain the concept of this technology, because people use facial recognition everyday in their personal interactions.

There are several reasons that known check fraudsters would be targeted for watch list screening rather than customers for a verification process. The smaller size of the check fraudster population makes it much more manageable than the customer population. There are perceived Personal Identifiable Information (PII) concerns, however only the face would be involved in an information exchange with another bank. Since a person's face is generally available at all times to the public, legally mandated constraints around information sharing are largely not applicable. Another reason is that it would be a monumental task to enroll all the "good guys."

There has been industry interest in developing facial recognition technology for fraud management purposes, but it is more focused on the customer than the fraudster. While there are many studies and surveys about biometrics in general, specific application of facial recognition to reduce fraud by targeting check fraudsters involved in one – on – one over-the-counter transaction is a new application of the technology. This paper explores the novel use of facial recognition as a tool to identify fraudsters committing over-the-counter check fraud at financial institutions.

Statement of the Problem

Given the current maturity level of computer assisted biometric facial pattern recognition, the ability of the technology to identify a person in a bank who is about to or has begun to conduct a fraudulent transaction from an internally developed fraud suspect watch list is in question. In a perfect world the identification of the person on the watch list would match 100 percent of the time and the transaction would be stopped. Since the perfect world does not exist, there are inherent challenges to using the technology as described by this research including:

- Accuracy of the technology -- Accuracy cannot be expected to be at 100%. However, it is expected that the product will produce results that are at 90% or better
- Timely notification -- Time is a perishable asset. The value of a timely notification can plummet to zero in the absence of an efficient dissemination of actionable information. The email alert system has to work as designed.
- Responsiveness of the investigator -- This is a critical component of the project. The investigator has to be able to assess the alert, determine a match, and call the branch to have positive impact.
- Knowing how to respond -- Overreaction and under reaction can both cause credibility issues for the project. The investigator has to know when it is appropriate to call law enforcement or to just call the branch. The wrong call can lead to litigation.

- Camera and lighting conditions -- Using existing camera equipment can be a risk. For facial recognition systems to work properly the cameras need to be focused, have light filters for natural light glare, and be targeted correctly. Artificial lighting needs to be adequate and steady with no flickering.
- False positives -- False positives are to be expected. How they are handled will be the challenge. Good quality suspect photographs combined with steady environmental (lighting) conditions and properly functioning cameras will aid the investigator in false positive analysis.
- False Negatives -- Missing a fraud event can have a negative impact on the project. An analysis of any false negatives will be necessary to see if the criminal adapted to the technology or the technology did not work.
- Privacy and civil liberties concerns -- One statement to the media that the technology has captured a person's identity can have a negative impact on the project. Clearly articulated policies that explain how the technology works and how the collected information will be used if prepared in advance, can address this concern.
- Criminal Inventiveness -- Criminals tend to be adaptive to new technology and can be inventive as they develop methods to defeat technology, including:
    - Active countermeasures to defeat protected targets.
    - Identifying soft or non protected targets.
    - Social engineering to passively undermine protected targets.

The research presented in this paper details the effectiveness of using a facial recognition system in a bank to prevent fraudulent transactions.

Using Biometrics

Biometrics is the use of biological or behavioral characteristics to uniquely identify a person. The word biometrics comes from the Greek bios (life) and metrikos (measure) (Jain, 2005). Biometrics, by their very nature, should be more reliable for identification purposes since they are unique to the individual. Any set of characteristics of a person can be used as a biometric, provided the feature satisfies the following four conditions (Jain, Ross, & Prabhaker, 2004).

- Universality – Every person should have those characteristics.
- Uniqueness – No two persons should be the same, in terms of those characteristics.
- Permanence – The characteristics should be invariant over time.
- Collectability – Quantitative measurement of the characteristics should be possible.

In a report for the European Parliament Committee on Citizen's Freedoms and Rights, the Institute for Prospective Technological Studies expanded on the four

conditions by adding three additional ones. Known as the "Seven Pillars of Biometric Wisdom" the report lists the following: (Maghiros et al., 2005)

- Universality – All human beings are endowed with the same physical characteristics – such as fingers, iris, face, DNA – which can be used for identification,
- Distinctiveness – For each person these characteristics are unique, and thus constitute a distinguishing feature,
- Permanence – These characteristics remain largely unchanged throughout a person's life,
- Collectability – A person's unique physical characteristics need to be collected in a reasonably easy fashion for quick identification,
- Performance – The degree of accuracy of identification must be quite high before the system can be operational,
- Acceptability – Applications will not be successful if the public offers strong and continuous resistance to biometrics,
- Resistance to Circumvention – In order to provide added security, a system needs to be harder to circumvent than existing identity management systems.

The three additional conditions were added to address expectations that the biometric system would work as advertised, be accepted by society, and have obvious enhanced security over existing technology being used for the same purpose.

It is suggested that biometrics has four basic uses: law enforcement, physical access control, (including the border), logical access control, and convenience (Maghiros et al., 2005). The primary use of biometrics today is to control access to secure facilities. A general requirement at a Wells Fargo data center is a single person mantrap controlled with a personal identification number (PIN) and hand geometry reader. The happiest place on earth, Disneyland, uses a fingerprint scanner to keep track of season pass holders. At the 1996 Olympic Games 65,000 athletes used hand geometry readers to gain access to event venues. In the e-commerce world low cost digital cameras are provided to customers to validate their on line transactions using facial recognition technology. The Simplifying Passenger Travel (SPT) program being tested at San Francisco International Airport uses a passenger's biometric information which links the passenger's frequent flyer number to the individual. Passengers in the SPT program use biometric scanners at unmanned self service kiosks to validate their identities, get their tickets, and check in. As long as the traveler has carry-on luggage, he is ready to travel (Group, 2004, #116).

Biometrics provides access to the virtual world by granting access to networks and data storage. MasterCard estimated that by using biometrics for online banking and point of sale transactions they would be able to cut fraud by 80 percent (Liu & Silverman, 2001). Fingerprint scanners are coming standard on

laptop computers to add an extra layer of protection and secure the device from unauthorized users. Wells Fargo in 1998 used facial recognition technology at unmanned kiosks in branch banks to cash payroll checks for non-customers.

The Rampart division of the Los Angeles Police Department recently provided field officers with hand held mobile personal data assistants (PDAs) equipped with facial recognition technology and pre-loaded with a list of wanted persons and gang members. The officers can use these PDAs in field situations to identify wanted persons who might otherwise provide false information about their identities (eWeek, 2004). The United States Army is studying the use of biometrics to provide better and more convenient security for access to their information and weapons systems (*Can Biometrics Help the Army Solve An Identity Crisis?* 2001). Some counties in the U.S. are using fingerprints embedded in Smart Cards to validate enrollees in entitlement programs.

In countries with literacy problems biometrics are used to provide banking services. Standard Bank of Africa has enrolled 500,000 people in their biometric program. Once enrolled, the customers can use Automated Teller Machines (ATM's) equipped with touch screen fingerprint scanners which then provide them access to financial services which they did not have before (Withers, 2002).

While the majority of the biometrics industry and government entities in the United States are focused on our borders and e-commerce, there is still work to be done in other areas. John Woodard, Jr. interviewed senior managers at the Department of Defense (DoD) to gauge their understanding of the use of biometric technology. Those interviewed were current and former political appointees, Senior Executive Service and General Officers, DoD employees, representatives from the Federal Bureau of Investigation (FBI) and the National Institute of Standards & Technology (NIST), as well as academic experts. Woodward summarized his interviews as follows, "In reviewing the biometric literature, one is struck by the limited amount of information describing how potential implementers and users perceive the technology" (Woodward, 2004). This suggests a lack of forward thinking and innovation in how to use these new tools.

As a regulated industry, financial institutions are required to have "surveillance pictures that can be used effectively as evidence in criminal prosecutions" ("ATM Public Safety and Crime Control Act" 1999). Surveillance technology has transitioned from analog video recorders to digital video recorders. DVRs have allowed financial institutions to accumulate vast databases of pictures of persons conducting banking business and fraudulent acts. These DVR systems are connected over networks. They are also remotely searchable as long as you know what transaction and who you are looking for.

Facial Recognition Biometrics

Public acceptance and education is the key to any biometrics program to avoid misunderstanding the technology and its intended uses. It is important for the public to understand that the intended goal of using facial recognition is to reduce over-the-counter check fraud, not gather a large picture database of customers conducting banking business that can be used for other purposes. It is necessary to avoid "Function Creep" that is making sure that the pictures captured and stored are only used for their intended purpose (Jain, Pankanti, Prabhakar, Hong, Ross, & Wayman, 2004).

There are widely diverse views of facial recognition technology and its purported impacts on society. It is no secret that camera surveillance is all around us. Fast food restaurants, gas stations, day care centers, government buildings, and financial institutions use closed circuit television cameras with recording devices to capture many daily activities. Two Harris Polls, one taken shortly after September 11, 2001, and the other taken six month later provide information about the public's view of surveillance activities. The first poll was taken September 19 – 21, 2001. It reported that when asked about ten specific proposals for new surveillance powers, more than 90% of the public supported three of them, between 80% and 90% supported three or more, and the rest were supported by between 54% and 68% (Taylor, 2001).

> These proposals, with the percentages of those that support and oppose them, include the use of facial-recognition technology to scan for suspected terrorists by 86% to 11%. Closer monitoring of banking and credit card transactions by 81% to 17%, a national I.D. system by 68% to 28%, expanded camera surveillance on streets and public places by 63% to 35%, and expanded monitoring of cell phones and emails by 54% to 41%.

The poll that was taken six months later showed a slightly different view of having increased surveillance powers.

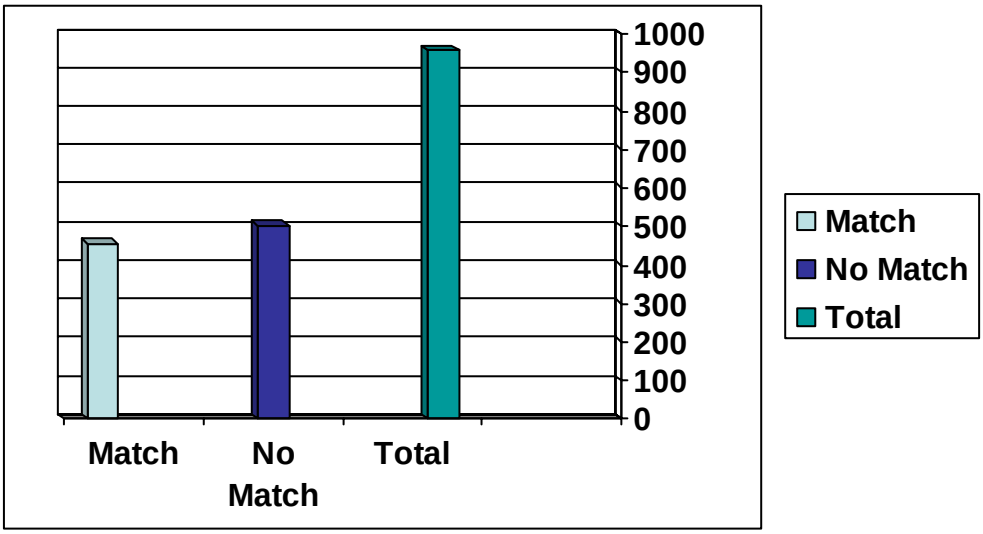
> Large majorities of the public continue to favor strong and expanded powers which law enforcement agencies might use when dealing with people suspected of terrorist activities. Use of facial recognition technology to scan for suspected terrorists at various locations and public events: favored by 81%, down from 86%. Closer monitoring of banking and credit card transactions to trace funding sources: favored by 72%, down from 81%. Adoption of a national I.D. system for all U.S. citizens: favored by 59%, down from 68%. Expanded camera surveillance on streets and in public places: favored by 58%, down from 63%. Expanded government monitoring of cell phones and email, to intercept communications: now favored by only 44% and opposed by 51% (Taylor, 2002).

While the differences are not significant, it is important to note that the second poll was taken only six months after the September 11 attacks. The modest decline is perhaps due to the lack of terrorist activities on United States soil. There was a major shift in public opinion in the area of how law enforcement is going to use the surveillance technology and if the use will be for its intended purpose.

Prior to 9/11 the general focus for facial recognition technology was on physical access control and claimed identity verification. In fraud management programs, the technology has been used to verify that a customer is who he purports to be instead of trying to match a fraudster's picture to a criminal watch list (Hirst, 2005). There is disagreement about whether or not the technology will even work for this purpose.

Facial recognition technology has an equal number of supporters and detractors. A test of facial recognition technology was conducted at the Palm Beach, Florida, International Airport March 11 through April fifteen, 2002. The Palm Beach County Department of Airports conducted two tests to discover the effectiveness of facial recognition technology in an airport checkpoint environment. Figure 1 shows the test data from the Phase 1 test summary (Airports, 2002, p. 3).

Figure 1. Facial Recognition Test Data Phase I

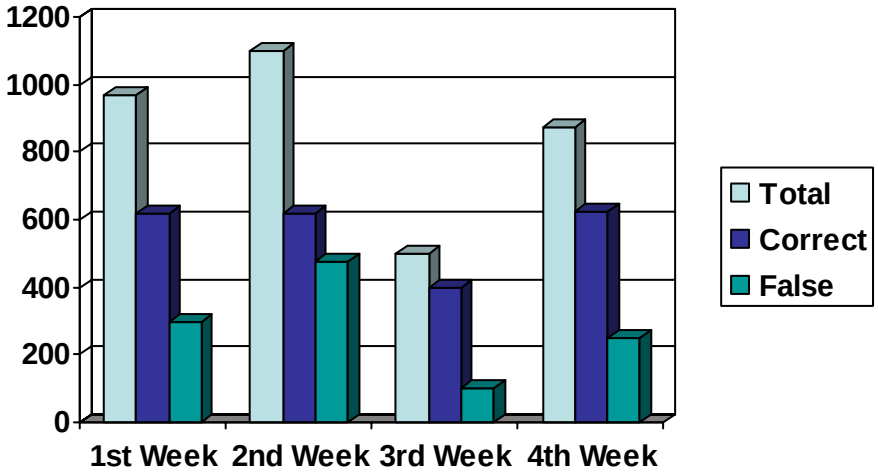


Source: Data collected from 15 Airport Employee Volunteers
Combined total attempts = 958 - Successful matches = 455 - Unsuccessful matches = 503

With almost a fifty percent failure or no match rate the American Civil Liberties Union (ACLU) reported that the technology did not work (Bowyer, 2004). Another way to view the results is that fifty percent of the time, persons enrolled in a watch list were detected by the system. Terrorists might rethink their objective if they believed that there was a fifty percent chance they would be detained.

Phase 2 tested the false positive and false negative rates. Basically false positives identity individuals who look similar but were not on the watch list and false negatives missed individuals who were on the watch list. The ACLU reported on the failure rate commenting that there were more than 1000 false alarms over four weeks of testing. This resulted in two to three false alarms per hour. During the test period multiple face captures were made of the 5000 ticketed passengers who passed through the test area which resulted in 10,000 total face captures. Figure 2 shows the Phase 2 test data for false alarms (Airports, 2002, p. 4).

Figure 2: Multiple alarms (both correct and false) on each alarm event



Source: Security Check point "through-put" traffic is approximately 5000 passengers per day. Average face capture rate is 10,000 per day.

The Palm Beach County Department of Airports report disclosed the following issues with the facial recognition technology used (Airports, 2002, p. 2).

> The data collected and compared to the manufacture's advertised specifications revealed the following:
>
> - Input photographs populating the database need to be of a good quality to avoid false alarms and insure successful matches.
> - Motion of the test subject head has a significant effect on the system ability to both capture and alarm on test subject.
> - There was a substantial loss in matching if test subject had a pose of 15 to 30 degrees (up / down, right / left) off camera focal point.

- Eyeglasses were problematic, glare from ambient light and tinted lenses diminished the system's effectiveness.
- System required approximately 250 lux of directional lighting to successfully capture faces and alarm on test subjects.

The Palm Beach County Department of Airports study raised questions about the facial recognition systems' ability to successfully make matches. The system relied on a single camera focused on a choke point through which travelers and employees had to pass. This technique may work in the retail branch bank as well. For the purposes of this research however, existing surveillance cameras that can capture faces from many angles were used to avoid creating a specialized test environment.

Privacy and Legal Concerns

Howard Rheingold wrote that "the average urbanite is caught on closed circuit television cameras 300 times a day" (Rheingold, 2002, p. 185). Motorola and Visionics announced, in March of 2002, their intention to develop a mobile device that would incorporate real – time facial recognition for law enforcement (Rheingold, 2002). The two companies were only minimally off in their timing. The Rampart Division of the Los Angles Police Department (LAPD) began using handheld devices to identify individuals in 2004. They have preloaded their mug book into a facial recognition system so that officers can use their hand held devices to compare a citizen contact with photos in their files. Luis Li, chief of the Los Angeles city attorney's criminal branch does not believe the technology will present privacy problems, because it is only used for identification. Li stated, "if you are standing in the street, you have no expectation of privacy" (eWeek, 2004).

The concern over personal privacy may be misrepresented because a person's face is always in the public. The ACLU worries about the misuse of facial recognition technology and at the same time suggests that the technology does not work. The ACLU seems to contradict itself. How can facial recognition be a threat to privacy if it does not work (Bowyer, 2004)? As technology has advanced, the United States courts have noted that it can shape their view of the constitution. Under 19th century constitutional application there was no need for law enforcement to get a warrant (Kopel & Drause, 2002). If someone from law enforcement was in a public place and was to overhear a conversation that resulted in an arrest, there would be no Fourth Amendment violations. Because of technological innovations, it became necessary for law enforcement to obtain warrants for its use in to gathering evidence in the analog and digital worlds. In a 1967 Supreme Court decision, *Katz v. United States*, they considered the issue where "evidence of petitioner's end of the conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the telephone booth from which the calls were made, was introduced at the trial" ("Katz v. United States 389 U.S. 347 " 1967). In essence the court in

this case decided that gathering evidence in a public place did not violate the defendants' rights. If Closed Circuit Television Systems (CCTV) is used in conjunction with a facial recognition system in public places there should be no expectation of privacy, as long as the cameras are in plain view.

Several states have passed or attempted to pass laws to address biometric identifiers. California, Connecticut, Nebraska, Pennsylvania, and Virginia put forth laws that would require a digitally embedded biometric identifier in drivers' licenses. The majority of these laws were not passed (Voit, 2005). New Jersey has passed legislation to protect biometric identifiers from being sold without the owner's consent. If the legislators understand what a primary biometric identifier is, then they may have acted in the best interests of their constituents. Preventing the sale of a person's photograph, fingerprint, or retina scan, which are considered primary biometric identifiers, is a positive move. Regardless, legal process in the form of a search warrant would make the biometric identifier available to law enforcement ("Biometric Identifier Privacy Act." 2002).

To date, the courts have provided no legal guidance on how facial recognition technology can be used by the government or the private sector in public places or private property (Bowyer, 2004). Everyone has a face and that face is readily visible virtually all the time a person is in public. Facial recognition technology still requires the human touch to validate the machine match. Theoretically, there is no difference between a convenience store, liquor store, gas station, or bank using CCTV to take pictures of patrons on private property and the LAPD's use of closed circuit cameras mounted in specially equipped radio cars to automatically search vehicles in public space at the rate of 1000 license plates an hour (LAPD Commander C. Beck, personal communication, April 5, 2005). The expectation of privacy is vanishing, for both individuals and their cars, whether in public or on private property.

The private sector has never had an issue with using closed circuit television cameras for surveillance purposes. In fact, private businesses are often sued for negligent security if they don't have surveillance cameras. As a deterrent to crime, private sector businesses even post signs warning that the premises are under camera surveillance. While the majority of businesses install surveillance cameras because of litigation fears and to be part of an "industry standard," financial institutions are required by regulation to have surveillance cameras (Scherer, 1989).

Media Confusion

The media at times misrepresents biometrics and in particular facial recognition technology. They overplay the success of the technology and exaggerate the potential for privacy violations. The public should be informed, but accurately. "America's Most Wanted," the successful television series, is a prime example of the positive use of the human ability to do facial recognition. Using Super Bowl

XXXV as an example of how the technology is misunderstood, the media quoted Representative Ed Markey, “It’s chilling, the notion that 100,000 people were subject to video surveillance and had their identities checked by the government” (Bowyer, 2004, p. 16). The Super Bowl fans did not have their identities checked by the government; their faces which were in the public were checked against a watch list of wanted persons.

The New York Times created more confusion when they reported after the Super Bowl that a woman in Texas who saw a picture of a man on television called the Tampa police to report that the man she identified owed back child support. Quoting the article, “It was the wrong person…The system is not 100 percent accurate” (Bowyer, 2004, p. 16). The woman saw the man’s face on television; this had nothing to do with the facial recognition system. As is often the case, the newspaper did not thoroughly research the incident before reporting it.

It was reported in 2004 that the Washington Elementary School District in Phoenix, Arizona, plans to install a facial recognition system in their district schools. Working with the Maricopa County Sheriff’s Office the district plans to create a watch list of sexual predators and runaway children. The system would alert school officials when there is a match to either a sexual predator or runaway student should they enter the school grounds (News, 2004). The ACLU is objecting to the use of facial recognition at the elementary schools on two grounds: 1) the technology does not work so there is no need to spend the money and, 2) there may be a risk of false alarms. The ACLU reported that the technology did not work 53 percent of the time when the Palm Beach County Department of Airports conducted tests in 2002 (Airports, 2002). Given those statistics the school district would probably rather err on the side of caution, than run the risk of a sexual predator getting onto the school grounds unchecked (News, 2004).

Methodology

This study focuses on determining if using a facial recognition system in a banking environment will produce more favorable results than other biometrics, as outlined above, in terms of accuracy, deterrence, and prevention.

Conceptual Framework

A three day operational test of the facial recognition system was conducted at fifteen separate branch banks. The goals of the field test were to obtain the following information: Can the facial recognition system match a person who has entered the branch bank to a picture of the person in the fraud watch list database? Can the facial recognition system generate consistent e-mail alerts to the investigations department.? Can any fraud deterrence or prevention advantage be gained by using the facial recognition system?

While there have been similar tests of facial recognition systems, the author has not discovered a test that encompasses what is proposed in this research. For these reasons the test was designed to reveal whether the facial recognition system is capable of producing the desired results as stated in the goals.

In addition to the three day test there was a 60 day pilot of the facial recognition technology to see how well it worked on the network and to determine whether actual fraud attempts could be identified. There were three groups for this test and pilot: fraudsters, bank robbers, and a control group of participants. The fraudsters and bank robbers were actual wanted persons who had criminal complaints filed against them with the local authorities. While the focus of this research is on fraud, bank robbers were added to provide more test data. The control group consisted of five participants to generate daily tests of the facial recognition and e-mail alert system over a three day period.

Product Selection

Facial recognition evaluation and testing primarily started in 1994 with the Facial Recognition Technology program (FERET). There were two additional FERET evaluations in subsequent years, 1995, and 1996. The FERET evaluations were mostly conducted on prototype systems at universities and labs. Grother, Bone, Blackbun, and Phillips designed the FERET evaluation model which became the NIST evaluation tool, as described in the article, “An Introduction to Evaluating Biometric Systems.” These initial tests were designed to automatically locate, normalize, and identify faces in a data base ("Face Recognition Technology," 2000).

The FERET tests by NIST were sponsored by the DoD Counterdrug Technology Development Program Office, Defense Advanced Research Projects Agency, and National Institute of Justice. The Facial Recognition Vendor Test (FRVT) was first conducted in 2000, when commercially available facial recognition products were making it to the market, and their claims needed to be evaluated. The sponsoring agencies and NIST changed their focus a little and decided to evaluate products already in or about to be introduced into the markets. The FRVT has become the benchmark and is generally cited in most research on facial recognition technology.

The FRVT 2000 test had two major goals for the evaluation. The first test was a technical assessment of capabilities of commercially available facial recognition systems. This was a test to determine the strengths and weaknesses of each individual system and discover the current state of the art for facial recognition (Blackburn, Bone, & Phillips, 2001). The second goal was to educate the biometrics community and the general public on how to present and analyze results. The authors of the report became aware that vendors and businesses preparing to use facial recognition technology were reporting exceptional success. These reported successes were made without understanding the

specifications and are virtually useless without knowing the details of the test that was used to produce the quoted results (Blackburn et al., 2001).

In the article, “Evaluating Technology Properly: Three Easy Steps to Success,” a three step process is recommended: technology evaluation, scenario evaluation and operational evaluation (Blackburn, 2001). The goal of the technology evaluation is to discover the technical capabilities of a specific test system. This testing is done in a controlled environment using a standard set of data that ideally has been collected universally. The technology tests should be repeatable and, depending upon the goals of the tests and size of the data sets, be able to be accomplished in a short time period.

Scenario testing differs from technology testing. Technology testing may just examine one facet of a facial recognition system, while scenario testing evaluates the entire system. Depending on the components of the facial recognition system, this might include the lighting system, the face capture and scanning system, the facial recognition operation system, and the data storage system. Scenario evaluation studies how well the entire system performs for a specific scenario (Blackburn, 2001). Scenario testing may test different system components, but the results should be the same. The evaluations may not be exactly reproducible, but the task should be repeatable.

Operational testing is done on location, using subjects in real life situations. Operational testing gives the evaluation valuable test data on system performance, strengths, and weaknesses. It typically is not reproducible because of dynamic field conditions and can last for several months. It is often stopped for several reasons. Perhaps an insufficient number of data sets passed through the test area or under field conditions the system simply did not work and required retooling, technological changes, and additional scenario testing.

In choosing a product for this project, it was important to consider the needs and the way in which solutions would be operationalized within the proposed test environment. The product had to be off-the-shelf technology and it was necessary to determine that it would operate as designed and as advertised. Another criterion was that the product could be easily installed and operated by investigators, with a minimal amount of training. The cost of the product was considered, but at this stage did not play a pivotal role because the potential impact that this technology might have on a fraud deterrence and prevention outweighed the expense.

The facial recognition technology product (FRT PRODUCT) selected for this study is 3VR Security, Inc., Intelligent Video Management System with integrated facial recognition analytics (3VR Security, 2006). This product purports to meet the criteria for off-the-shelf technology, but further tests are necessary to determine if the product works as advertised and can produce results.

Method of Analysis

Currently, facial recognition is considered fairly inaccurate. People change over time and the environmental conditions are erratic. Lighting conditions and the way people pose can influence the ability of the facial recognition system to capture the face in either a validation or identification process. There are also other factors to consider when evaluating a facial recognition system. Operationally it is important to consider acceptability, ease of data acquisition, ergonomic issues, and the time it takes for the enrollment and identification process (Maghiros et al., 2005). In reviewing the test results, the ability of the facial recognition system to produce the desired results was evaluated. An analysis of the test results was categorized by individual branch banks into the following categories:

- Acceptability
  - Did the product install and operate as advertised?
  - Was the technology accepted by users and supporters?
- Technical challenges
  - Environmental
  - Operational
  - Number of successful E-mail alerts
  - Number of false positives
- Operational Challenges
  - Number of frauds interrupted or stopped
  - Number of matches to actual suspects and the control groups

Success Framework

The ABA Deposit Account Fraud Survey Report estimates that the average loss per check fraud was $1,098 in 2003 (Association, 2004, p. 13) To measure Return on Investment (ROI), the average check fraud loss was analyzed on a per branch basis to determine the number of frauds that need to be interrupted or stopped to realize a return. Using the ABA average number of $1098 per event, the total number of frauds that need to be prevented are approximately 215 (see Table 1). The author has personally overseen the installation of bank branch camera surveillance systems and estimates the costs at $1000 per camera. These costs include the installation and a DVR. In the pilot, each branch required 16 cameras, for a total of $16,000 each. Facial recognition technology doubled the price to $2000 per camera for a total of $32,000 per branch. Pilot project costs were estimated to be $480,000, less typical surveillance system costs for a net expense of $240,000.

Table 1: ROI Check Fraud Average Loss per Event

15 Branch ROI	Average Loss Per Branch	Total Branch's in pilot	Average Check Fraud per Branch to Stop	15 Branch Total Check Frauds Needed to Stop
$240,000	$1098	15	14	215

Deterrence is just one of the fraud management processes. In the strictest sense, it is the number one process: deter the suspect and stop the fraud before it happens (Wilhelm, 2004). However, measuring the success of a deterrent activity, such as facial recognition technology, can present challenges. One component of the facial recognition system is the CCTV camera. Evaluating the deterrent effect of CCTV systems on crime has been the subject of many studies. There have been instances where non – operational cameras have been used to deter crime and had an impact. When CCTV systems are used together with other measures, as this project suggests, they are more effective (Deisman, 2003).

To measure deterrence, the fifteen branch banks were monitored for over the counter fraud events during the test period. Additionally, successive attempts by the same suspect(s) were tracked by number of tries.

Environmental Conditions

Facial recognition technology requires more stringent tuning of the cameras and lighting than the typical surveillance system in order to be effective. Prior to beginning testing of the FRT PRODUCT, each of the fifteen branches was surveyed and the survey data was assessed in several areas. Five data elements were measured. They are listed below with their respective definitions.

- Glare – Natural sunlight that shines into the branch through windows either directly behind the cameras or from side entrance windows and reflects sunlight on target surface areas.
- Obstructions – Design elements or safety equipment that the cameras shoot through to reach a target area.
- Camera Angles – Angles that are either optimal for FRT PRODUCT or that are considered less than optimal because they are positioned high relative to the target or to the far right or far left..
- Field of View –Optimizing the use of existing camera lens.
- Focus – Focus and quality of the camera.

The branches were surveyed after the installation of the FRT PRODUCT and the five data element measurements were assigned a class rating for each of the branches from one (low quality) to five (high quality). These measurements were used to evaluate the success of the FRT PRODUCT to detect targets and to develop a system whereby improvements could be made in order to enhance the detection ability of the FRT PRODUCT. A cost improvement structure was developed from the environmental assessment and improvements were made prior to system testing.

Notification and Alert Timeliness

Notification timeliness was analyzed by enrolling five participants into the FRT PRODUCT'S watch list at the branch level. Each of the five participants visited each branch 45 times over the three day period for a total of 225 visits. A notification cycle was determined to be the elapsed time from FRT PRODUCT detection of the target to when the related email alert was received by an investigator. This elapsed time was then compared to the time stamp generated by the teller system when the participants conducted a mock transaction. The time stamped document indicated whether the elapsed time from the initial detection to the email alert provided sufficient time for the investigator to intervene and disrupt the transaction.

FRT PRODUCT Accuracy

The five participants followed the same cycle of branch visits to test the FRT PRODUCT'S ability to accurately detect persons on the watch list. Participants entered a branch and simulated customer behavior by going to the check writing podium, filling out a document, moving to the queue line, and waiting for the next available teller. Once recognized by the teller, the participant went to the available teller window and presented the mock transaction document. The teller branded the document with date, time, branch reference number, and teller identification number. This document represented the mock fraud transaction and the overall elapsed time difference determined if the email alert was received in sufficient time by an investigator to have disrupted the transaction. The participant then exited the teller window and branch. For safety and security reasons both the participants and tellers knew about the test and were escorted by an investigator.

Results

The results of this research analyze the effectiveness of the FRT PRODUCT to target over the counter check fraudsters. The FRT PRODUCT tests are broken down into three elements.

1. Environmental conditions
2. Notification email alert timeliness test
3. System accuracy

Environmental Conditions

For the purpose of classifying the branches environmentally, it was necessary to develop a common criterion for evaluating the existing conditions relative to the cameras and the ability of the FRT PRODUCT to capture usable pictures. A set of terms was developed by the vendor and the author which, when applied to individual branches, classified the branch from one to five, with five having the most attributes for a successful match (3VR Security, 2006).

The branches were classified to develop a scoring method to indicate if the branch needed equipment enhancements or additional labor (e.g. camera angle adjustment) to bring it up to acceptable levels. The enhancements or labor add to the overall project cost. Table 2 shows how the branch quality level is defined by determination criteria which equates to a subsequent classification.

Some of the branches had a bandit barrier, which created an obstruction. A bandit barrier is a bullet resistant Plexiglas barrier that is approximately one and one-half to one and seven-eights inches thick and extends from the teller counter to ceiling. Bandit barriers are typically used in high robbery crime areas. Some of the branches required the camera to shoot through the barrier to the target.

Table 2 Branch Classification Criteria

Rank	Determination Criteria
5	No cutouts, no glare, good angles, field of view, and focus
4	Problems with one of the items listed above
3	Problems with two of the items listed above
2	Problems with three of the items listed above
1	Cameras out of focus, inadequately positioned

Branch Survey Results.

Each of the fifteen branches was surveyed to determine its environmental classification and to establish what additional costs would be required to bring it up to an acceptable level. Branches with acceptable levels have high match or hit rates and few false positives. Table 3 shows the post survey branch classification and subsequent costs for the modifications to achieve the quality rating.

Table 3 Classification and Associated Costs

Branch Reference Number	Classification	Equipment Costs	Labor Costs	Cost Per Branch
611	5	$1,107	$1,800	$2,907
701	5	$1,750	$2,160	$3,910
855	5	$1,194	$2,160	$3,354
740	4	$2,440	$2,160	$4,600
851	4	$750	$1,440	$2,190
765	4	$1,150	$2,160	$3,310
652	4	$637	$2,160	$2,797
296	4	$1,715	$2,160	$3,875
863	4	$1,845	$1,449	$3,294
609	4	$675	$1,440	$2,115
599	3	$1,425	$1,440	$2,865
879	3	$1,000	$1,440	$2,440
188	3	$4,114	$4,320	$8,434
433	2	$600	$1,080	$1,680
396	2	$300	$1,440	$1,740
	Totals	$20,702	$28,809	$49,511

In some instances the costs to bring a branch to a class of three, for example, was deemed too high to warrant the expenditure. Other branches were at an acceptable or higher level because of recently installed equipment not related to this project.

Post Modification Image Results

Four branches were selected to demonstrate the classification criteria (see pictures in Appendix A). Reference branch 611 had a classification of five. This location produced an image with no glare, had good angles, good field of view, good focus, and did not require the cameras to shoot through the bandit barrier. Reference branch 609 had a classification of four. This location produced an image with no glare, moderately poor vertical camera angles, good field of view, good focus, and the cameras shot through the bandit barrier, but effectiveness was not reduced. Reference branch 599 had a classification of three. This location produced an image with no glare, moderately poor vertical camera angles, poor field of view, and the bandit barrier created obstructions in the target area. Reference branch 433 had a classification of two. This location had no glare, significantly poor vertical camera angles, good field of view, good focus, and the bandit barrier had an impact due to built in obstructions in the target area. Vertical angle had more of an impact than glare, field of view, or focus.

Notification Timeliness

Timeliness is a critical component of the FRT PRODUCT results evaluation. Timeliness for this project was measured by the elapsed time from the point of detection by the FRT PRODUCT to the receipt of the email alert by the investigator. This is the time span necessary for the FRT PRODUCT to detect the participant in the branch, compare and match the participant, and send an email alert to the investigator. The success measurement is that the FRT PRODUCT does this very early, so that the investigator has time to review the alert and then implement a transaction disruption strategy with the branch staff to prevent a fraudulent transaction. Five watch list test participants were sent to all fifteen branches on three different days. The operational test simulated persons on a watch list wanted for a fraud crime. The test participants were instructed to enter the branch, pause at the check writing podium to fill out a deposit slip, and wait in the queue line for the next available teller. Once called to the teller window the test participant would hand the document to the teller and the teller would brand the document with date, time, teller number, and reference location number. This document would be retained by the author for future use in the timeliness evaluation. One hundred thirty four email alerts were generated out of 225 expected. For the purpose of this test, an email alert is defined as when the FRT PRODUCT generates an email alert on one of the enrolled participants and sends it to an investigator.

Timeliness Test Issues

One of the test participants dropped out after the first day. This resulted in fewer opportunities to capture a picture of the test participants. Slightly less than fifty percent of the branch email servers did not function on day one of the three day test, resulting in no email alerts being sent. This lowered the number of available alerts to evaluate. There could be more email alerts than participant visits. The FRT PRODUCT is programmed to send an alert each time a participant is recognized by the FRT PRODUCT. This could result in multiple alerts per participant at each branch as s/he traveled throughout the branch and his/her face was captured by the FRT PRODUCT. Each time the face was matched, an alert was expected to be generated. While some email alerts were not sent, they remained on the FRT PRODUCT server in queue to be sent. This occurred at the branches that experienced email server problems.

Table 4 shows the number of watch list alerts generated by branch with corresponding elapse time, from time of detection to the receipt of the email alert by the investigator. Times are reflected in hours, minutes, and seconds. Branches with zero elapsed time did not detect the participant prior to the time of mock transaction.

Table 4 Email Alerts with Elapsed Time

Branch Reference Number	Watch List Alerts	Average Elapsed Time
855	13	0:00:30
701	12	0:00:52
611	12	0:02:15
851	9	0:00:00
863	10	0:00:00
296	6	0:00:00
652	7	0:00:43
609	11	0:01:36
765	10	0:00:00
740	13	0:00:20
879	10	0:00:12
599	11	0:02:53
188	8	0:02:38
396	2	0:03:00
433	0	0:00:00
Total Alerts	134	

Transaction Branding

Transaction branding times were used to determine if the test participants could be intercepted at the teller window based on initial detection time. A minimum target time difference was set at three minutes. This would give the investigator three minutes to assess the match, develop a disruption strategy, and call the branch. Table 4 shows the single longest branding time recorded by branch. These are single events and those three minutes and over met this test goal.

Table 5 Single Longest Transaction Branding time

Branch Reference Number	Single Longest Transaction Branding Time
855	3:00
701	3:00
611	6:00
851	0:00
863	0:00
296	0:00
652	2:00
609	5:00
765	0:00
740	1:00
879	1:00
599	12:00
188	4:00
396	6:00
433	0:00

Approximately fifty percent of the branches scored below the minimum three minute threshold on a single event basis and in general no branch demonstrated a consistent branding differential which met stated goals.

FRT PRODUCT Accuracy

In order to be successful in operational test accuracy, the FRT PRODUCT needed to produce accuracy results equal to or greater than ninety percent. The FRT PRODUCT in this test produced an average hit rate of sixty three percent which is shown in Table 6. Individually, the class five branches scored ninety five percent which exceeded the expected results.

Day one testing had the feature comparison setting sensitivity set at eighty percent. Feature comparison settings were adjusted from eighty percent on day one to sixty five percent on day two and three. The higher the feature comparison setting the more exact the person has to match the stored image. The lower the setting the more latitude the system has to make a match.

Table 6 – Operational Test Success Rate Three Days of Testing

Branch Reference Number	Alerts	Tries	Hit %	False (+)	Total Faces	False (+) %	False (-)	False (-)%
	Class 5 Branches							
855	13	13	100%	3	8179	0.04%	0	0.00%
701	12	13	92%	1	11048	0.01%	1	7.69%
611	12	13	92%	4	11292	0.04%	1	7.69%
Subtotal	37	39	95%	8	30519	0.03%	2	5.13%
	Class 4 Branches							
851	9	13	69%	4	15547	0.03%	4	30.77%
863	10	13	77%	0	5052	0.00%	3	23.08%
296	6	13	46%	0	2831	0.00%	7	53.85%
652	7	13	54%	0	4143	0.00%	6	46.15%
609	11	13	85%	0	6706	0.00%	2	15.38%
765	10	13	77%	1	7668	0.01%	3	23.08%
740	13	13	100%	1	7434	0.01%	0	0.00%
Subtotal	66	91	73%	6	49381	0.01%	25	27.47%
	Class 3 Branches							
879	10	12	83%	1	10566	0.01%	2	16.67%
599	11	12	92%	5	5934	0.08%	1	8.33%
188	8	13	62%	3	4073	0.07%	5	38.46%
Subtotal	29	37	78%	9	20573	0.04%	8	21.15%
	Class 2 Branches							
396	2	13	15%	8	2142	0.37%	11	84.62%
433	0	13	0%	0	2300	0.00%	13	100.00%
Subtotal	2	26	8%	8	4442	0.18%	24	92.31%
Totals	134	193	63%	31	104915	0.07%	59	30.57%

Lower settings produced better results. Day one hit results were forty seven percent, day two results were eighty five percent, and day three results were eighty two percent. Also, the higher the environmental class rating the better the results. Class five branches on day two and three scored one hundred percent hit rates. Appendix B shows day one through three results on an individual day basis.

False Positive Analysis

Every face captured or recorded is an opportunity for a false positive. Biometric samples can contain multiple images. The number of faces captured does not necessarily equal the total number of images. According to a paper published by

the National Institute of Standards and Technology titled *The NIST HumanID Evaluation Framework (HEF)* (Micheals, Grother, & Phillips, 2003, p.2),

> In the HEF model, the following terminology describes biometric information at different grouping levels. Each human subject of interest is an individual. A collection of biometric data for a single individual makes up a signature. A collection of signatures constitutes a signature set.

In this example of the HEF model, each image, or in this case each signature, is counted when calculating total faces in the database. Following the HEF reasoning, the number of false positives was calculated against total faces captured. Table 6 shows the false positive rates for the three day test period and Appendix B shows the false positives at the daily level. The results were at an acceptable level.

False Negative Results

The false negative rate, the number of times that the participants were not detected by the FRT PRODUCT, was higher than expected. Fifty nine false negatives equates to a thirty percent chance that the fraudster was able to complete a fraud.

Discussion

There were three main tests in this project; 1) Environmental, which evaluated the existing camera equipment and natural and artificial lighting conditions at fifteen branches to determine if the FRT PRODUCT would work; 2) Timeliness of alerts, which was tested to determine if the FRT PRODUCT could match a person on the watch list to a live person in the branch and alert an investigator in time to take some action to prevent a fraud from occurring; and 3) Accuracy of the FRT PRODUCT, which evaluated FRT PRODUCT'S ability to successfully match persons on a watch list to the live person when they entered the branch.

Several real fraud suspects were enrolled in the watch list at the beginning of the testing period, however none came into the branches during the test period. As important as it was to be looking for real fraudsters, there would be no guarantee that any of them would appear in one of the fifteen branches. In order to get test results with simulated real conditions, five participants were hired by the vendor. The five participants were enrolled in the FRT PRODUCT system as fraud suspects and a watch list was created. The participants visited each branch on three separate days. The data gathered from the test watch list subjects is what was used to evaluate timeliness and accuracy.

Environmental

The first step in the process was to survey the fifteen branch locations to evaluate their camera equipment and lighting conditions. It was necessary to conduct the surveys in order to determine if the facial recognition system could function as designed under existing conditions. Early on it was revealed that the cameras were of sufficient quality, but were either out of focus, lacked glare guards, or were mounted at an angle that prevented facial recognition from working. There were no artificial lighting issues during the testing period.

Initially when researching this project, a product was sought that was advertised to work with existing branch surveillance cameras. The existing cameras had been installed to primarily capture pictures of subjects who were engaged in fraud or bank robbery crimes. When applying the FRT PRODUCT, it was discovered that the cameras were not focused precisely as required by the FRT PRODUCT. Angles were often too high (vertically) and prevented the FRT PRODUCT from capturing a full on face. Glare from daylight washed out many of the cameras, which, along with reflected glare from tile floors, created conditions that were unacceptable.

All of these issues were addressed to varying degrees and branch equipment was brought up to acceptable levels where possible. In some instances the cost to raise the quality was not justified. Each of the fifteen branches was assigned a numerical ranking from one (low) to five (high) after the necessary enhancements were made.

For this FRT PRODUCT to work at its best, an almost horizontal plane from the subject's face to the camera was necessary. This attribute was a rarity, as all the cameras were ceiling mounted and had some degree of downward angle on the subjects. Certain behavioral patterns of the customers were observed. Customers looked left to right more often than they looked up and down. This observation added weight to the theory that vertical height with increased angle impeded successful matches. People seldom looked up at ceiling mounted cameras. For this reason, vertical angle was deemed a critical criterion.

There was a major reliance on channeling customers to the queue line where they were staged with a well focused camera. When watch list test subjects posed at the head of the queue line, not only were good pictures obtained, but successful matches were made.

Bandit barriers played a role in how well the FRT PRODUCT performed. Several of the branches had older style bandit barriers which use a metal voice box that the teller and customer use to communicate with each other. Ceiling mounted cameras with a downward angle generally placed the voice box in the facial area of the target. At times this had a negative impact on the FRT PRODUCT'S ability to capture a face at the teller window. This impact was not deemed too

important, as there were many opportunities to capture a face from the multi-camera system. Newer style bandit barriers use an offset Plexiglas overlay instead of the metal voice box for communications and this had little or no impact on the FRT PRODUCT, unless the target was standing directly in line with the offset. Bandit barriers are typically placed in bank branches that are in high crime areas.

The average cost to bring the fifteen branches up to a workable level was $3,290 each. The original intent was to install an FRT PRODUCT that would work with the existing equipment. By utilizing the FRT PRODUCT, better picture quality was achieved overall. Issues that had been overlooked or generally accepted were corrected and a better understanding of what is required to get better quality pictures was achieved. Future camera system installations will use what was learned in this project and better standards will be employed.

Timeliness

Timeliness was deemed a critical measurement for this project. The ability of the selected FRT PRODUCT to identify the target and make timely notification was measured by the time elapsed from the time the FRT PRODUCT detected the watch list subject in the branch to when the email alert was received by the investigator. A minimum acceptable time was set at three minutes. This would give the investigator time to examine the two pictures, watch list enrollment photo and real time photo of the target in the branch, and take some action to disrupt the fraud transaction.

Several things impacted this test. It was anticipated that at any financial institution branch bank there would be some level of customer activity that would generally slow down the fraudster before s/he reached the teller. After interviewing branch staff, it was learned that the 2006 World Cup Soccer games unexpectedly lessened the numbers of customers in the lobby during test periods. There was reduced lobby traffic on the test days. The fewer customers allowed the test participants to literally walk into the branch, fill out a deposit slip, and go directly to the teller window. This contributed to a short speed to target time and all but eliminated the possibility for any intervention.

There were four systems used to capture and calculate time; 1) the FRT PRODUCT server, 2) the DVR server, 3) the teller server, and 4) the email server. These systems are not synchronized with each other. The teller and email server track time to the nearest minute while the FRT PRODUCT and DVR server track time to 1/100th of a second. The least significant was the teller and email servers, so all times were tracked to the minute. The teller and email server round time so that an alert sent by the FRT PRODUCT at 09:05:57 AM matched against a teller transaction time of 09:06:02 AM will indicate one minute between alert and completion of transaction. Also if times are within the same

minute even though they may be 50 seconds apart, it will show that the alert and transaction occurred simultaneously.

While timeliness of the alerts is an important feature, giving the investigator time to react is far more important. None of the branches achieved a consistent three minute window from time of alert to when the target reached the teller window. There were single events noted that met this criteria, but overall the majority of the targets would have reached the teller window before the investigator could have taken any action. To further validate the time issue, each of the participants passed a deposit slip to the teller for branding. Once branded with date, time, branch reference number, and teller number the deposit slip was returned to the participant. The deposit slips were collected and are being kept for further analysis.

The timeliness issues which surfaced indicated that in order to get the three minutes necessary to react to the alert, there needs to be better positioning of the cameras, so that the individuals are captured when they first enter the branch. Basically a camera gauntlet needs to be set up so that everyone who enters the branch is caught by the FRT PRODUCT as soon as possible.

Accuracy

The five participants (less the one dropout) were enrolled in the FRT PRODUCT'S watch list and visited the fifteen branch banks on three separate days to test the FRT PRODUCT. It was observed that these individuals looked into cameras more than other bank customers. This could have skewed the alert results, as the participants overacted in the operational test. For safety and security reasons it was necessary for all parties involved to know about the project. For five individuals to enter a branch bank and begin conducting mock transactions this could have caused concerned employees to notify law enforcement or worse, activate a hold-up alarm.

Branches with better tuned cameras and lighting scored higher In looking at the four examples in Appendix A, reference locations 611, 609, and 599 have a better vertical angle on the targets while reference location 433's vertical angle looks down on the subject more steeply. In branch 433 the distance from the teller line target area to the camera was shorter than the other branches and this made it difficult to lower the camera for a better angle. Because this was a grocery store branch, there was limited room to lower the cameras. If they had been lowered, they would have become physical obstructions and aesthetically unacceptable. Grocery store branches will require further research in order to improve their accuracy.

False Positives

There are different ways to evaluate false positives. One idea suggests that human appearances, not "faces," contained in the database represent the measurement for false positives. For example if 2,000 images are captured representing 100 people and five false positives are generated out of the 100 people, then the false positive rate is five percent. Human appearance numbers were not available for this test.

The other idea suggests that for every face capture there is an opportunity for a false positive alarm. Using the same numbers in the above example the false positive rate would be five out of 2000 or .25%.

During the test period the participants visited the branches 193 times. Since there were more than 193 total human appearances during the test period, this figure is not representative of the total population. However, in the second theory the FRT PRODUCT captured a total of 104,915 faces of which 31 false positives alert emails were sent. In this evaluation there would have been a 0.07% false positive rate.

In reviewing the Face Recognition database, there are multiple databases for researchers to use depending upon what type of facial recognition tests they might be conducting. In each of the sub-databases, the population is described as being a series of individuals with multiple pictures of the same person. One example lists 1199 individuals and 365 duplicates for a data set of 1564 which was used nine times to produce 14,126 images (Grgic & Delac, 2005).

For the purpose of this research the author chose the method that every face capture represents an opportunity for a false positive theory, which produced a false positive rate of 0.07%.

False Negatives

False negatives are those instances when the participant was in a branch and the FRT PRODUCT failed to identity them. While false positives can be a nuisance, false negatives represent a failure to recognize a fraudster enrolled in the watch list and worse yet, mean the fraudster was able to enter the branch and presumably commit an over the counter fraud crime. These rates were exceptionally high given the fact that the participants knew about the test they were involved in. There was no attempt to avoid the cameras or conceal their faces and in most instances they posed at the teller window and smiled at the camera.

Comparative sensitivity settings played a role in reducing the false negatives. When the settings were lowered from 85% to 65% there was a marked improvement from a false negative rate of 50% on day one to below 20% on

days two and three. Still the false negative rates were unacceptably high and further research needs to be conducted to determine the cause.

Conclusion

This research project proposed the use of facial recognition as a technology to disrupt over the counter check fraudsters before they can complete their crime. There were many parts to the project that required equipment to work with precision in order for responders to be successful. The camera system had to be tuned for optimal functionality in terms of glare, focus, and angle.

The operational tests provided satisfactory recognition rates with good confidence measures. The good confidence measures indicate that this technology could be useful in identifying fraudsters before they are able to commit their crime. The operational tests proved that 70 % of fraudsters could be detected by the facial recognition system.

The operational tests also showed that 30 % of the fraud transactions would have gone undetected by the facial recognition system. This false negative rate was caused by excessive camera angles and older cameras that could not accept improvements to glare and focus problems.

The timeliness of the detection operational test left no time for a response plan to be implemented. This means that 100% of the time the test participants would have succeeded with their fraud crimes had they been real crooks and the response team would have been notified as they were walking out the door. This test identified that more study is required to understand how to better place cameras to identify people earlier as they enter the branch. The tests also demonstrated that email alerts may not be the best way for notification and that a more localized system is needed if branch staff are going to have a chance to disrupt the fraudulent transaction.

Future Work

For facial recognition to work in real – world situations, there needs to be more importance placed on camera positioning and angles. Since the primary purpose of using facial recognition in this project was to disrupt a fraudulent transaction, there is a need to develop strategies that will enable earlier detection. Once earlier detection is developed, operational tests can be run again to observe response plans and measure their potential for success.

As was shown earlier, successful hit rates can be increased by decreasing the similarity confidence levels which will ease the strict match requirements of the FRT PRODUCT. Doing this before implementing the technology in actual

conditions would boost the possibility of earlier successes, rather than troubleshooting and adjusting when hits are missed.

Initial camera surveillance system installation should be improved to incorporate the needs of facial recognition technology. Just decreasing the vertical angle to the target can offer significant improvement in system performance. One possible option would be to develop installation standards that would start with facial recognition system requirements and install surveillance systems based on those standards.

The results of this study indicate that facial recognition systems have the potential for reducing fraud in over the counter transactions. What is needed is earlier detection of the fraudster as they enter a branch. Earlier detection gives branch staff time to react and respond to the fraudster before s/he can complete their crime.

About the Author

Gary S. Reynolds, CFE is Director of Financial and Electronic Crime Investigations in the Corporate Security group at Wells Fargo. Having spent 20 years in law enforcement, Gary has been involved in the detection and prevention of fraud in a variety of situations and cases. Gary's reputation as one of the experts in this field is widely recognized. He has been involved in cases that include bank fraud investigation, white collar crime investigation, consumer fraud investigation, real estate fraud investigation, and high technology crime investigation. Since having joined Wells Fargo, Gary has been involved in domestic and international investigations involving bank fraud and high technology crimes. Gary also manages the Executive Protection function and is a member of the company's Threat Assessment Team for both physical and cyber threats. He is also a member of the company's Privacy Council.

Gary is a member of the Association of Certified Fraud Examiners where he obtained certification. He is also a member of the High Technology Crime Investigators Association, USSS Electronic Crime Taskforce, Infragard, American Society for Industrial Security, the Institute of Internal Auditors, and is on the board of the Financial Services Information Sharing and Analysis Center (FS/ISAC). Gary manages a team of 54 professional investigators for Wells Fargo.

Gary holds a Bachelor of Arts degree in Public Service Management from the University of Redlands, and a Master of Science in Economic Crime Management from Utica College.

References

3VR Security, I. (2006). *Intelligent Video Management for Retail Banking*. San Francisco, Retrieved April 15, 2006, from http://www.3vr.com/files/Banking%20Whitepaper.pdf

Abagnale, F. (2005, May 4). *Identity Theft.* Paper presented at the Financial Services ISAC Members Meeting, St. Petersburg, Florida.

Airports, P. B. C. D. (2002). *Statistical report regarding facial recognition technology testing at Palm Beach International Airport*.

Association, A. B. (2004). *ABA Deposit Account Fraud Survey Report 2004*. Washington D.C.: American Bankers Association.

ATM Public Safety and Crime Control Act, 106th CONGRESS, 1st Session (1999).

Biometric Identifier Privacy Act., STATE OF NEW JERSEY ASSEMBLY, 210th Sess.(2002).

Blackburn, D. M. (2001, July). Evaluating Technology Properly: Three Easy Steps to Success. *Corrections Today,* 5.

Blackburn, D. M., Bone, M., & P. Jonathon Phillips, P. D. (2001). *Facial Recognition Vendor Test 2000*.

Bowyer, K. W. (2004). Face Recognition Technology: Security versus Privacy. *IEEE Technology and Society Magazine,* 14.

Can Biometrics Help the Army Solve An Identity Crisis? (No. RB-3024 (2001))(2001). No. RB-3024 (2001)): Rand Arroyo Center.

Deisman, W. (2003). *CCTV: Literature Review and Bibliography*. Ottawa: Research and Evaluation Branch Community, Contract and Aboriginal Policing Services Directorate, Royal Canadian Mounted Police.

eWeek. (2004). LA Police Dept. Studies Facial Recognition Software. Retrieved June 4, 2005, from http://infotrac-college.thomsonlearning.com/itw/infomark/612/1/67971137w5/purl=rcl-W

Face Recognition Technology. (2000). Retrieved June 14, 2005, from http://www.frvt.org/default.htm

Grgic, M., & Delac, K. (2005). FACE RECOGNITION

Group, S. I. (2004). Simplifying Passenger Travel (Spt). *Executive Brief* Retrieved April 8, 2006, from http://simplifying-travel.org/files/SPT_Executive_Brief_01_JUN04.pdf

Hirst, C. (2005). *A Primer on Biometric Technologies* (No. G00126307): Gartner, Inc.

Jain, A. (2005). Biometrics. Retrieved May 18, 2005, from http://encarta.msn.com/text_1741500789_1/Biometrics.html

Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., & Wayman, J. L. (2004, August). *Biometrics: A Grand Challenge.* Paper presented at the Proceedings of International Conference on Pattern Recognition, Cambridge, UK.

Jain, A. K., Ross, A., & Prabhaker, S. (2004). An Introduction to Biometric Recognition, *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image-and Video-Based Biometrics* (Vol. 2005, pp. 29): IEEE.

Katz v. United States 389 U.S. 347 (U.S. Supreme Court 1967).

Liu, S., & Silverman, M. (2001). A Practical Guide to Biometric Security Technology, *IT Professional* (pp. 9): IEEE Educational Activities Department.

Maghiros, I., Punie, Y., Delaitre, S., Lignos, E., Rodriguez, C., Ulbrich, M., & Marcelino, C. (2005). *Biometrics at the Frontiers: Assessing the Impact on Society* (No. EUR 2158 EN). Spain: Institute for Prospective Technological Studies.

Micheals, R., Grother, P., & Phillips, P. J. (2003). The NIST HumanID Evaluation Framework. Retrieved July 29, 2006, from http://www.frvt.org/DLs/AVBPA-2003.pdf

News, E. T. (2004). Plan to use facial recognition software draws criticism from civil rights group. *Child Safety* Retrieved June 4, 2005, from http://infotrac-college.thomsonlearning.com/itw/infomark/612/1/67971137w5/purl=rcl_W

Norton, R. E., & Ryan, R. (2005, May 4, 2005). *Biometrics and identity Assurance.* Paper presented at the Financial Services ISAC Member Meeting, St. Petersburg, Florida.

Press, T. A. (2005). Tampa police eliminate controversial facial-recognition system*. USA Today*.

Rheingold, H. (2002). *Smart Mobs* (First ed.). Cambridge: Perseus Book Group.

Scherer, E. (1989). Split-Second Security. *Security Management, 33*(51), 1.

Taylor, H. (2001). Overwhelming Public Support For Increasing Surveillance Powers And, In Spite Of Many Concerns About Potential Abuses, Confidence That These Powers Would Be Used Properly. *THE HARRIS POLL #49, October 3, 2001* Retrieved May 1, 2005, from http://www.harrisinteractive.com/harris_poll/printerfriend/index.asp?PID=260

Taylor, H. (2002). Homeland Security. *THE HARRIS POLL® #16, April 3, 2002* Retrieved May 3, 2005, from www.harrisinteractive.com/harris_poll/index.asp?PID=293

Tucker, L. (2003). Gotcha! *Science World* (pp. 5): Scholastic, Inc.

Voit, B. (2005). State Anti-Terrorism Legislation. *Suggested State Legislation Docket Items* Retrieved April 8, 2006, from http://www.csg.org/CSG/Programs/suggested+state+legislation/anti-terrorism+legislation.htm

Westin, D. A. (2003). New Survey Shows Public Willing to Accept Biometric Identifiers, But Demands Privacy Safeguards. Retrieved May 17, 2005, from http://www.pandab.org/biometricsurvey.html

Wilhelm, W. K. (2004, Spring). The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management, *Journal of Economic Crime Management*. Retrieved August 16, 2004, from http://www.utica.edu/academic/institutes/ecii/publications/articles/BA309CD2-01B6-DA6B-5F1DD7850BF6EE22.pdf.

Withers, S. (2002, July 2). Biometrics special: Who are you? *Technology & Business*.

Woodward Jr, J. D., Horn, C., Gatune, J., & Thomas, A. (2003). Biometrics A Look at Facial Recognition. Santa Monica, California: RAND.

Woodward Jr., J. D., Orlans, N. M., & Higgins, P. T. (2003). *Biometrics*. Berkeley: McGraw-Hill/Osborne.

Appendix A

Reference Number: 611

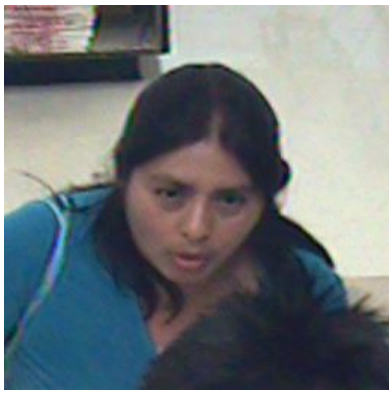
Environmental Classing: 5

Reference Number: 609

Environmental Ranking: 4

Reference Number: 599

Environmental Class: 3



Reference Number: 433

Environmental Class: 2

Appendix B

Day One Results

Branch Reference Number	Alerts	Tries	Hit %	False (+)	Total Faces	False (+) %	False (-)	False (-)%
Class 5 Branches								
855	5	5	100%	1	2622	0.04%	0	0.00%
701	4	5	80%	0	3818	0.00%	1	20.00%
611	4	5	80%	1	3350	0.03%	1	20.00%
Subtotal	**13**	**15**	**87%**	**2**	**9790**	**0.02%**	**2**	**13.33%**
Class 4 Branches								
851	2	5	40%	0	5223	0.00%	3	60.00%
863	3	5	60%	0	1805	0.00%	2	40.00%
296	1	5	20%	0	1016	0.00%	4	80.00%
652	0	5	0%	0	1425	0.00%	5	100.00%
609	3	5	60%	0	2263	0.00%	2	40.00%
765	2	5	40%	0	2661	0.00%	3	60.00%
740	5	5	100%	0	2919	0.00%	0	0.00%
Subtotal	**16**	**35**	**46%**	**0**	**17312**	**0.00%**	**19**	**54.29%**
Class 3 Branches								
879	2	4	50%	0	3590	0.00%	2	50.00%
599	3	4	75%	0	2118	0.00%	1	25.00%
188	0	5	0%	0	1196	0.00%	5	100.00%
Subtotal	**5**	**13**	**38%**	**0**	**6904**	**0.00%**	**8**	**58.33%**
Class 2 Branches								
396	0	5	0%	0	737	0.00%	5	100.00%
433	0	5	0%	0	820	0.00%	5	100.00%
Subtotal	**0**	**10**	**0%**	**0**	**1557**	**0.00%**	**10**	**100.00%**
Daily Total	**34**	**73**	**47%**	**2**	**35563**	**0.01%**	**39**	**53.42%**

Day Two Results

Branch Reference Number	Alerts	Tries	Hit %	False (+)	Total Faces	False (+) %	False (-)	False (-)%
Class 5 Branches								
855	4	4	100%	0	2799	0.00%	0	0.00%
701	4	4	100%	0	3229	0.00%	0	0.00%
611	4	4	100%	1	4205	0.02%	0	0.00%
Subtotal	**12**	**12**	**100%**	**1**	**10233**	**0.01%**	**0**	**0.00%**
Class 4 Branches								
851	4	4	100%	4	5120	0.08%	0	0.00%
863	4	4	100%	0	1710	0.00%	0	0.00%
296	2	4	50%	0	880	0.00%	2	50.00%
652	4	4	100%	0	1334	0.00%	0	0.00%
609	4	4	100%	0	2308	0.00%	0	0.00%
765	4	4	100%	0	2355	0.00%	0	0.00%
740	4	4	100%	1	2259	0.04%	0	0.00%
Subtotal	**26**	**28**	**93%**	**5**	**15966**	**0.03%**	**2**	**7.14%**
Class 3 Branches								
879	4	4	100%	1	3263	0.03%	0	0.00%
599	4	4	100%	0	1687	0.00%	0	0.00%
188	4	4	100%	1	1145	0.09%	0	0.00%
Subtotal	**12**	**12**	**100%**	**2**	**6095**	**0.03%**	**0**	**0.00%**
Class 2 Branches								
396	1	4	25%	1	578	0.17%	3	75.00%
433	0	4	0%	0	664	0.00%	4	100.00%
Subtotal	**1**	**8**	**13%**	**1**	**1242**	**0.08%**	**7**	**87.50%**
Daily Total	**51**	**60**	**85%**	**9**	**33536**	**0.03%**	**9**	**15.00%**

Day Three Results

Branch Reference Number	Alerts	Tries	Hit %	False (+)	Total Faces	False (+) %	False (-)	False (-)%
Class 5 Branches								
855	4	4	100%	2	2758	0.07%	0	0.00%
701	4	4	100%	1	4001	0.02%	0	0.00%
611	4	4	100%	2	3737	0.05%	0	0.00%
Subtotal	**12**	**12**	**100%**	**5**	**10496**	**0.05%**	**0**	**0.00%**
Class 4 Branches								
851	3	4	75%	0	5204	0.00%	1	25.00%
863	3	4	75%	0	1537	0.00%	1	25.00%
296	3	4	75%	0	935	0.00%	1	25.00%
652	3	4	75%	0	1384	0.00%	1	25.00%
609	4	4	100%	0	2135	0.00%	0	0.00%
765	4	4	100%	1	2652	0.04%	0	0.00%
740	4	4	100%	0	2256	0.00%	0	0.00%
Subtotal	**24**	**28**	**86%**	**1**	**16103**	**0.01%**	**4**	**14.29%**
Class 3 Branches								
879	4	4	100%	0	3713	0.00%	0	0.00%
599	4	4	100%	5	2129	0.23%	0	0.00%
188	4	4	100%	2	1732	0.12%	0	0.00%
Subtotal	**12**	**12**	**100%**	**7**	**7574**	**0.09%**	**0**	**0.00%**
Class 2 Branches								
396	1	4	25%	7	827	0.85%	3	75.00%
433	0	4	0%	0	816	0.00%	4	100.00%
Subtotal	**1**	**8**	**13%**	**7**	**1643**	**0.43%**	**7**	**87.50%**
Daily Total	**49**	**60**	**82%**	**20**	**35816**	**0.06%**	**11**	**18.33%**