AN EXPLORATION OF USING FACE RECOGNITION TECHNOLOGIES FOR NATIONAL SECURITY

Yüzden Tanıma Teknolojisinin Ulusal Güvenlik Alanında Kullanılması Üzerine Bir Çalışma

Ahmet S. YAYLA*
Samantha K. HASTINGS**

Özet

Teknolojinin ilerlemesi ile birlikte, günlük hayatımızda daha geniş imkanlara ve avantajlara sahip olmaktayız. İste, Yüzden Tanıma (Face Recognition) metodu da henüz gerçekleşen bu gelişmelerden birisidir. Eğer usulüne uygun olarak kullanılırsa, yüzden tanıma metodu insanların ve polis teşkilatlarının gündelik hayatlarına devrim niteliğinde yenilikler ve kolaylıklar getirecek ve özellikle de polis teşkilatlarının rutin islerini daha etkili ve hızlı hale gelmesini sağlayacaktır.

Bu çalışma yüzden tanıma metodu üzerinde durmakta ve geçmişten günümüze yüzden tanıma metodunu incelemektedir. Yüzden tanıma metodunu inceleme çalışmaları sırasında yüzden tanıma metodunu test amacı ile gerçek hayattan alınan fotoğraflar ile yüzden tanıma metodu test edilmiştir. Test neticeleri bize yüzden tanıma metodunun gelecek için çok iyi imkanlar sunabilecek bir uygulama olduğunu ortaya koymuştur. Olumlu ve cesaretlendirici test neticeleri bizi Yüzden Tanıma metodu uygulamaları içeren iki yeni proje üzerinde çalışmaya sevk etti. Bu bağlamda yüzden tanıma metodunu kullanarak kaybolan çocukları bulmaya yönelik bir program ve yine ayni metodu kullanarak ulusal çapta Türk Polis Teşkilatı tarafından uygulanabilecek olan bir güvenlik ve kovuşturma aracı geliştirilmesi ve kullanılması projeleri üzerinde çalışılmaktadır.

Anahtar Kelimeler: Yüzden Tanıma, Ulusal Güvenlik, Terörizm, Dijital Fotoğraf, Tahkikat, Güvenlik.

Abstract

The more the technology advances, the more advantages and opportunities we have in our daily lives. Face recognition is among one of those recent advancements. If used properly, face recognition can be a revolutionary instrument in our lives, in particular for law enforcement.

* University of North Texas, ayayla@lis.admin.unt.edu
** Dr., Interim Dean, University of North Texas, Hastings@lis.admin.unt.edu

This study focuses on the use of face recognition and its history from the beginning until today. As we continued to investigate the value of face recognition, we tested a number of real life pictures by using a face recognition system. The results of our experimentation hold great promise for future applications of face recognition. Additionally, encouraged by the results of our testing, we have begun to work on two new face recognition projects. We are investigating the use of face recognition in finding missing children and we are also launching an extensive nationwide implementation of face recognition-based investigation and security tools for law enforcement in Turkey.

Key Words: Face Recognition, National Security, Terrorism, Digital Images, Investigation, Security.

Introduction

The more the technology advances, the more advantages and opportunities we have in our daily lives. Face recognition is among one of those recent advancements. If used properly, face recognition can be a revolutionary instrument in our lives, in particular for law enforcement. This study focuses on the use of face recognition and its history from the beginning until today. As we continued to investigate the value of face recognition, we tested a number of real life pictures by using a face recognition system. The results of our experimentation hold great promise for future applications of face recognition. Additionally, encouraged by the results of our testing, we have begun to work on two new face recognition projects. We are investigating the use of face recognition in finding missing children and we are also launching an extensive nationwide implementation of face recognition-based investigation and security tools for law enforcement in Turkey.

Face Recognition

Face recognition was one of the earliest methods of identity verification. The face has been one of the simplest and almost effortless ways to get information about identity, race, sex and age as well as expressions and emotions throughout history (Lyons et al., 1999). Today, with the help of advanced computer technology, the earliest method of identification has become the most sophisticated and a state-of-the-art instrument of identity verification for security. For the last two decades researchers have focused on the opportunities for computerized face recognition using biometric technology.

Face recognition technology is commonly being used for two main applications. The first and the most common applications are primarily put into practice by law enforcement agencies. Through out the world, law enforcement agencies and the military use face recognition technology for security purposes in the airports, at the borders, for public safety purposes, in prisons, for mug shot albums and for real-time video surveillance purposes. In addition, commercial companies use facial recognition systems for a variety of applications including security and access purposes. Commercial uses range from static photo (still facial images like mug

shots) and face matching on credit/ATM cards, passports, driver licenses and photo ID to real time matching with live faces, video images or still images. There are many commercial businesses using facial recognition technology in their daily business practice in financial applications, casinos and gaming industry, and for security purposes.

What is Face Recognition?

Face recognition, in its simplest definition, is getting people's identities from images by using specially designed computer algorithms (Yang et al., 2002). Face recognition is the process of comparing one or a series of input images against a known database of images and alerting the users if there is a match between the input and database images (Sung and Poggio, 1998). Face recognition works by using biometrics technology simply by employing computerized methods to recognize or verify the identity of a person based on his/her physiological characteristic on digital images or videos (Gao and Leung, 2002). The immediate frontal view of face including eyes, eyebrows, mouth, chin, nose and their interrelation between themselves including the distance between them are usually used to generate an algorithm as unique as face which allows comparison between the faces (Jia and Nixon, 1995). There are usually two general major tasks in face recognition. The first is locating the faces in entered images and the second is recognizing those located files (Hong and Jain, 1998).

Why Face Recognition?

The human face has many advantages for recognition when compared with the other means of identity verification such as finger print and retina scan. First of all, everybody has a unique and distinct face with many inherent features. Then, the face is readily available and does not require contact with the subject (Jia and Nixon, 1995). Face recognition can be processed without disturbing or stopping the subject in a "hands-free way" (Chien and Wu, 2002). Therefore, it is much easier to get a picture of somebody instead of getting a finger print or a retinal scan because face recognition offers the advantage of being a non-intrusive and passive method to authenticate personal identity in a natural and friendly way (Gao and Leung, 2002). Face recognition is also less expensive than other traditional and biometric verification systems. A solid and reliable face recognition system can be built by using low-cost computers and cameras which are readily available almost everywhere.

History of Face Recognition

One of the earliest studies about face recognition belongs to Teuvo Kohonen. In his book "Self-organization and Associative Memory", published in 1988, the author tried to demonstrate that neural a net could be used in recognizing faces from aligned and normalized face images. Kohonen tried to compute a face description formula by approximating the eigenvectors of the face images. Today, eigenvectors are known as "eiganfaces". Even though Kohonen's system was not successful, his study was a starting point for other researchers. He demonstrated the need for

accurate alignment and normalization (Pentland and Choudhury, 2000). Later, Kirby and Sirovich in their work, published in 1990, described a compact and usable representation of facial appearance (Kirby and Sirovich, 1990). In 1991, Turk and Pentland demonstrated the first facial identification process by using eigenface representation (Turk and Pentland, 1991). They were especially effective in real-time pattern recognition techniques that are the bases of todays face recognition technology (Edwards et al, 1997).

As recently as 1993, even though there were some studies and important findings, facial recognition was usually considered a technology that would probably never work efficiently in the real world. However, the Department of Defense (DOD) Counterdrug Technology Development Program Office's Face Recognition Technology Program (FERET) managed to change that opinion by conducting numerous development efforts, data collection and evaluations (Bone and Crumbacker, 2001). In 1993, seeing the successes of several research projects in different universities creating facial recognition algorithms and facial recognition applications, the FERET program started in the September of 1993, in the Army Research Laboratory in Maryland. The goals of FERET were to lead a research to develop automatic facial recognition system that would assist security, intelligence and law enforcement personnel in their daily tasks. The program consisted of three major parts. The initial task was the selection of the research that would be a part in the program. The second phase was the collection of the FERET Database. Consequently, FERET targeted the evaluations of the algorithms that were used to test FERET Database.

In the first phase, FERET awarded the research grants to:

- Massachusetts Institute of Technology (MIT), Alex Pentland
- Rutgers University, Joseph Wilder
- The Analytic Science Company (TASC), Gale Gordon
- University of Illinois at Chicago (UIC) and University of Illinois at Urbana-Champagne, Lewis Sadler and Thomas Huang
- University of Southern California (USC), Christoph von der Malsburg

In the second phase, MIT, TASC, and USC were granted to continue development of their algorithms. There was an obvious need for a large database of images to test the algorithms. Before FERET, most databases were small and the number of available images was limited. The FERET database was completed in three years. The researchers collected 1564 sets of pictures for a total of 14,126 images that belonged to 1199 different individuals with 365 duplicate sets of these images. Duplicate images were mostly modified images or images that were taken on a different day. For some images, over two years elapsed between the first and second picture taken (FERET, 2003).

The FERET program was highly successful. The research was successfully completed in 1998. This research yielded creditability and provided direction to the researchers and companies in the area of facial recognition. The database and the results of the research were made available on the internet to the researchers. Soon after this research was completed, a number of private companies began to provide

applications of facial recognition system based on the facial recognition algorithms that were used in FERET project.

Examples of the Currently Used Systems

After the mid 1990s, with new advancements in biometrics technology, the old traditional way of identification by face has become the newest way of ID verification and security systems.

Citywide facial recognition system was first used in the United Kingdom in 1998. London Borough of Newham was the first city that installed 140 security and surveillance cameras to implement a facial recognition system in the city. The main purpose of the project was to fight against criminals (Silva, 2002). After one year, the city officials announced that crime rate dropped more than 40 percent. Of course, it is not clear whether the crime rate dropped because cameras were visible and the public were aware of the face recognition system or because criminals thought their faces could be caught by the face recognition system (Rothstein, 2001). In January 14, 2002, it was announced by the authorities that the facial recognition system had identified a wanted person in the United Kingdom where the facial recognition system was utilized citywide for security purposes (Telecomworldwide, 2002).

Video cameras and face-recognition technology were used during the January 2001 Super Bowl in Raymond James Stadium to search the crowd streaming through the turnstiles for known criminals and/or terrorists (Rothstein, 2001). Each and every fan's face was captured by a camera that was connected to a police camera control room inside the stadium to compare against 1,700 images of known criminals and terrorists. At the end, over 100,000 people were scanned and 19 people matched to the photos of known criminals. However, no one was arrested (Hindus, 2001). In addition to the stadium experience, Tampa police installed 36 surveillance cameras in Tampa's entertainment district Ybor City in mid-summer in 2001. The police aimed to run the faces of people scanned on the streets against the face records of 30,000 wanted terrorists, felons and missing children in their database (Rothstein, 2001). Similarly, Virginia Beach Police installed thirteen cameras at the beachfront for security purposes. Three of the cameras were hooked up with a facial recognition system to screen the crowds on the pavements and beachfronts (McGuire, 2002).

The facial recognition system was used at Winter 2002 Olympic Games at Utah Salt Lake City to protect the gold medals. The main purpose was to ensure the clearance into medal's storage area (Kerber, 2002).

The U.S. Federal Government including the U.S. Immigration and Naturalization Service (INS), the National Security Agency (NSA), the U.S. Army Research Laboratory, and the National Institute of Justice are already using face recognition based security systems (Washington Post, 1998). According to Oliver Buck Revell, the former Associate Deputy Director of the FBI, over one hundred security systems equipped with facial recognition software in the United States, the United Kingdom, Canada, and Mexico, including Britain's National Crime Squad (NCS), more than 50 RCMP detachments and police departments across Canada, and in over 40 police

departments across the U.S. are currently being used successfully (Imagis, 2003). The INS' SENTRI Project is a good example of the implementation of face recognition systems by the governments. This system was developed by INS to provide rapid transportation for commuters across the US/Mexico border. People who don't want to wait at the border gate security check points simply apply to INS to enroll in the SENTRI program. Approved commuters are permitted to use a fast lane to cross the border into the United States. The commuters are issued a radiofrequency (RF) tag that is attached to their vehicle by the INS that lets the system identity commuter as they approach the border gates. The tag codes store a unique identification (ID) number for the authorized persons and vehicles. Each ID number includes a facial digital photograph taken at the time of the enrollment. As the vehicles enter the border gate, facial recognition system automatically captures the face of the person and compares it with the previously created record. If the facial recognition formulas match, the vehicles are granted to proceed without delay. If the system denies access, the vehicles are automatically routed to an inspection station (INS SENTRI, 2003).

In 2000, the state of Illinois cross checked the pictures of people in the driver license database by using face recognition software and surprisingly and successfully found multiple driver licenses issued to a single person (Clark, 2002).

In Tallahassee, Florida, the Department of Highway Safety and Motor Vehicles is considering the use of face-recognition technology as a security measure to reduce the number of fake driver licenses in the state. The authorities in Tallahassee estimate that there are tens of thousands phony driver licenses currently issued by their city. In this regard, senators approved to include a section that allows the motor vehicle agency to implement the use of biometric data such as face-scanning technology into antiterrorism legislation that could be passed during the 2003 legislative session in Florida. Sen. Ginny Brown-Waite, R-Brooksville, Fla., chairman of the Senate's public security and crisis management committee announced that ``It would give us yet another method of verifying that a person who presents themselves is who they say they are" (Clark, 2002).

The Colorado Department of Motor Vehicles, under a bill approved by state lawmakers in 2001, was scanning driver's license photographs into a database that is currently being compared with new photos taken for licenses after July 1, 2002 (Kelsey, 2001). West Virginia Department of Public Safety also uses such a system in an effort to reduce the numbers of phony driver licenses (Buckler, 1997).

Currently, hundreds of casinos are using facial recognition security systems for security purposes around the world which are claimed to be working very efficiently. Here is a real incident that recently occurred in Canada. A young elegantly dressed blond woman entered into a Gateway Casino in Vancouver, British Columbia, Canada. She immediately sat down at a black jack table and played a few hands. So far everything seemed quite normal. However, suddenly up in the security room an alarm went off, where the face recognition system was scanning the faces of people in the casino against known criminals. The stylish young woman was identified as a person with several prior convictions for pick-

pocketing in Vancouver, Los Vegas and the Bahamas. The Security began to follow the stylish lady from distance to make sure that she was there just for gambling. The blond woman joined the crowd, and slowly slipped her hands in a woman's purse and pulled out her wallet. The victim of picket-pocketing was focused on her growing pile of chips and she wasn't aware that her purse was stolen. Eventually, the pickpocket was caught before she left the casino and the woman got her purse back. Casino security personnel handed the pick-pocketing woman to the police along with the pickpocket incident on tape (Hindus, 2001).

New ATM machines will no longer require card or identification numbers. Instead, they will rely on face-recognition technology. The machine will take a digital photo of the user's face during his or her visit to the ATM machines, and verify the user's identity by comparing the latest photo with a running record of photo database recorded by the banks (Stock, 2000). Currently, check-cashing company Mr. Payroll, Inc. in Fort Worth, Texas, is using this system. The biometric face recognition technology is now actively being used in about 42 check-cashing ATMs in convenience stores and warehouses throughout the Southwest, United States. According to the company, the system has almost completely eradicated fraud at those machines and strengthened customer confidence (DiDio, 1998). In addition, more than 40 Italian banks are using security systems based on face recognition technology. The Italian bank security systems serve as a high-security access control system. A person trying to enter an area secured with this technology is held in a small room between the bank's entrance and main lobby until the face recognition system verifies the person's identity (American Banker, 1999).

Airports Using Facial Recognition System for Security Purposes

Thunder Bay International Airport is the first airport to utilize a facial recognition based security system in Canada. The facial recognition system at Thunder Bay International Airport is used to gain access to the secure areas in the airport. According to the officials, facial recognition system let them use their resources more efficiently and deploy security personnel more effectively. The system works with a swappable ID card and a wall mounted camera. As the user swipes the card, the facial recognition system verifies the identity in less than a second through the camera installed mounted on the wall. The system is claimed to be working very effectively. According to the authorities at Thunder Bay International Airport, the false acceptance rate was 0% meaning that unauthorized users were never let in. However, the false rejection rate was 3.1%, which means that authorized users were denied access only 3.1% of the time (Delaney, 2002).

The Dallas-Forth Worth, (DFW) airport began to test a face recognition system for security purposes at the beginning of January 2002. At the DFW airport, the face recognition system is used to catch suspicious passengers before they board planes. The system at DFW was set on medium sensitivity. The security system using facial recognition at DFW yielded a 94 percent correct alarm rate and 1.5 percent false alarm rate (Gips, 2002). Also, Iceland's Keflavik International Airport has signed a contract to install a security system using face recognition technology. Boston Logan

International Airport and California's Fresno Yosemite International Airport have begun to test face recognition technology since September 11th (Harrison, 2002).

In November 2002, Qantas air security team started to evaluate the face recognition technology at Sydney Airport. The system works by reading the passport pictures and comparing that picture with the person at the gate. The Qantas staff places their passport on a reader and the passengers look into a fixed camera. The face is then compared with the passport photograph. If the passport picture and the face match, security gates to the aircraft opens automatically. This process takes only about 10 seconds (Mills, 2003). In addition to the Sidney airport, New Hampshire's Manchester Airport has also begun to implement face recognition system to enhance security and safety of the travelers in 2002 (Viisage, 2002).

Face Recognition and Law Enforcement

Face Recognition technology has numerous advantages for law enforcement during their daily practices in the fight against terrorism, narcotics, or other. In general, face recognition technology does not require extra sources and effort for law enforcement. First of all, the images that can be used for face recognition is readily available as the process of law enforcement is strictly related with images whether for identity purposes or crime scene investigation. Law enforcement agencies already have their picture archives available even though those pictures were not intended to be used for facial recognition. In addition to the law enforcement archives, a picture of a suspect or fugitive can easily be acquired through a variety of sources such as driver license records, school IDs and albums, family pictures etc. Also, security and surveillance systems are rich sources for getting images. Therefore, it is relatively easy for law enforcement to get a picture of somebody if needed for an investigation.

In addition to available pictures, almost all of the law enforcement agencies either have or have access to cameras and computers. The majority of the agencies have their own computer networks, and they are connected each other through the special networks or over the internet. Facial recognition systems work on regular computers without extra updates or requirements. Usually computers that are used by the law enforcement agencies in their daily tasks have enough computer power to process the images for facial recognition systems. Therefore, facial recognition technology does not require new hardware unless it is desired by the agencies or users.

One of the other positive aspects of facial recognition systems is that they are user and subject friendly. Face recognition systems work in a hands free way where the law enforcement does not need to touch the subjects and where the subjects are not disturbed by the process. Unlike the finger print and retina scan, face recognition systems do not disturb the subjects in any way. Furthermore, because face recognition systems do not require more than loading the pictures, they are reasonably easy to use for users.

Testing Face Recognition at the Texas Center for Digital Knowledge (TXCDK)

Our study began with two unique plans. The first project is to establish a new nation wide security and investigation tool based on facial recognition systems for law enforcement in the country of Turkey. The second project is the foundation of the new International Center for Finding Missing and Runaway Children. The primary mission of this center is finding and locating missing and runaway children by using the facial recognition technology against the missing children's picture database.

Turkey and Face Recognition

Even though, facial recognition based security and investigation systems are currently being used around the world, currently there aren't any countries that are using this system nationwide like Automated Fingerprint Identification Systems. The main purposes of the nationwide automated facial recognition system that will be established in Turkey is enhancing security and providing new tools to law enforcement in the fight against terrorism and crime.

Implementation of a nationwide facial recognition based security system in Turkey is relatively easy as Turkey has a variety of advantages regarding this matter. First of all, Turkey has only one National Police Agency. The jurisdiction of Turkish National Police includes all of the big cities, towns, airports and highways. Unlike other countries and other police agencies, Turkish National Police (TNP) oversees all of the criminal activities and security measures regardless of the crime type. Not only does TNP fight against terrorism, organized crime, regular street crimes and others, but also it has specialized units for each type of crime along with the appropriate investigation tools such as ballistics and forensic laboratories. Additionally, the security and protection of all of the airports and seaports in Turkey is provided by TNP. Furthermore, TNP is the only authorized agency for issuing driver licenses and passports. This exceptional structure of TNP provides unique advantages for the implementation of a nationwide facial recognition system. The database for the proposed facial recognition system is already readily available through the criminal and suspect mugshots, driver license and passport picture databases in the headquarters of the TNP.

The second and maybe the most important factor in the implementation of face recognition based system in Turkey is the TNP Computer Network, which is named POLNET. POLNET is the nationwide special police network that connects all of the Turkish National Police Divisions including the headquarters, police stations and substations, airport, harbor, train station police, or any police building around the country regardless of the size. As of now, POLNET is the largest Microsoft based network in the world. Additionally, this network is fast enough to transmit pictures and videos simultaneously without any additional upgrade. One of the other advantages of POLNET is that it is a secure network without external or internet connections. The Turkish Police uses another independent network just for Internet access which secures its POLNET network from outside intrusion. The implementation of a face recognition system on the already available Turkish POLNET is rather easy and does not require vast budget sources.

Turkey's geo-political position is also an important aspect for such project. Turkey connects Europe and Asia and is located in the middle of Asia, Europe and Africa just to the north-west of the Middle East. Because of Turkey's geographical location, many criminals including drug dealers and terrorists try to use Turkey as a bridge between the Europe and Asia for their illicit activities. Drug dealers generally attempt to transport prohibited drugs through Turkey. Terrorists use Turkish airports very often to connect with other flights. Therefore, Turkey is subject to a heavy traffic of international criminals most of whom use phony IDs or passports. A Face Recognition system working through the security cameras at the airports and borders that scans the faces of passengers and people who enter Turkey against a known international criminal and terrorist database will help to catch criminals or people that are trying to use phony IDs or passports.

Missing or Runaway Children, Face Recognition and the International Center for Tracking Missing Children on the Internet

Currently, authorities estimate that at least 100 million children are missing worldwide (Inministry, 2003). In 2001, approximately 850.000 children were reported missing to the authorities in the United States (FBI-NCIC, 2003). The missing children data statistics include the children who were abducted, thrownaway, runaways, lost, injured and otherwise missing children.

It is usually quite difficult to find the missing children. It generally takes time and tremendous effort and resources to track missing children. Sadly, very often, missing children fall in the hands of criminals and become material for illicit activities. Crime cartels and rings use children for dealing drugs, theft and sex trade. Unfortunately, young girls are usually at the risk of being lured into sex trade. Missing young girls are frequently prostituted or used as child pornography objects.

There are a large number of both national and international agencies that collect information and pictures on missing children. For example, Interpol maintains a database of missing, abducted and runaway children on behalf of the 181 Interpol member countries (Interpol, 2003). In addition to Interpol, the FBI keeps a database of missing children in the U.S. Besides the formal government agencies, non profit organizations also try to keep information in order to try to find the missing children.

Face recognition systems are a useful and effective tool to track the missing children by using the readily available database especially in child pornography cases. The missing children that are the victims of child porn can be located easily by using the missing children's databases against the child porn materials on the internet with the help of a face recognition system. Our International Center for Tracking Missing Children on the Internet at the University of North Texas is established for the purpose of helping the missing children and their families. Our initial goal is to gather the missing children database in our center and load the pictures of missing children into the face recognition system. In the second step, we will begin to gather the pictures of child pornography victims and load those pictures into our system. We will run these two databases against each other and try to find

the matching pictures. This process will be a continuous task as we get more pictures of both missing children and the children that are the victims of child pornography. As we match the pictures, law enforcement agencies will be contacted in order to let them know about the match.

Facial Recognition Experimentation

We tested facial recognition at the University of North Texas TXCDK Digital Imaging Computer Laboratory. We installed face recognition software on a video workstation. The video workstation was a Pentium 3 based computer with single 850 MHz CPU and 256 megabytes of memory.

The data for the experimentation came from the Turkish National Police. We used the mugshots from real terrorist events. We preferred to use actual data in our testing as this system is going to be used by Turkish National Police by using similar images in the near future. We used 140 pictures for this study. All of the pictures were randomly selected from different police cases that took place during the recent years. The pictures included both male and female subjects. There were pictures where the subjects were wearing eye glasses or where the subjects had facial hair. Subjects in the pictures had long and short hair. Some of the subjects were facing their right or left less than approximately 30 degrees. In one single picture, the subject was facing 90 degrees left. 49 of our pictures were in color and 91 of the pictures were black & white. Most of the pictures were developed through a professional film laboratory whereas some of the pictures were printouts from digital images or just plain photocopies. We scanned the pictures that we got them as paper mugshot pictures. We scanned the pictures in 400 dpi resolution and saved them as "gif" files. After we digitalized the mugshots, we loaded them into our system.

The software we used required the pictures either automatically aligned or manually aligned before the pictures are used for comparison. As the pictures are aligned, the system scores overall image quality based on the following criteria:

- Details of the picture
- Head-size
- Cropping of the head from the original picture
- Brightness
- Darkness
- Focus
- Eyes
- Glare

As the system scores the images, it also asseses each image in terms of image quality by labeling them as:

- Poor
- Fair
- Moderate
- Good
- Excellent

As we aligned the pictures, the system labeled our pictures in our experimentation database as follows:

Table 1: Quality Distribution of Pictures

Quality	Number of the Pictures (General)	Number of Color Pictures
Poor	17	0
Moderate	42	14
Fair	40	11
Good	13	3
Excellent	28	21
Total Images	140	49

The image scores given by the face recognition software also proved that our database represented a variety of options that reflect real life cases. The database was homogenous in terms of picture quality. The color pictures tended to get better scores from the system. Even though, some of the color pictures were scanned, they scored better than some of the black and white pictures. The images that were labeled less than good commonly had brightness and focus problems. Even thought those pictures with problematic focusing and brightness had good head cropping, glare and well aligned eyes, they were scored less than excellent or good because obviously the brightness and focus was affecting the face recognition process negatively. Later on as we ran the pictures against our database, we realized that the pictures with focusing and brightness problems got lower scores from the recognition process also.

After we aligned the pictures in our database, we began to test the face recognition process. We ran each picture one by one against the other 140 pictures in our database. The system scores the recognition process as it recognizes each picture based on the recognition. It gives up to ten alternative pictures with relevant scores. In our testing, the system recognized successfully all of our 140 pictures. The recognition ratio was 100% which means that all of the pictures were matched exactly to the same person's pictures. However, only 65 of 140 pictures were scored 10 out of 10. (Table 3). The rest of the pictures' scores varied from 9.99 to 7.91. The mean score for all of the pictures was 9.84. (Table 1). One of the pictures was scored 7.91 because the subject in that picture was facing 90 degrees right. One of the eyes was missing in the picture. So, it was scored less than the others. The lowest score with two eyes in the picture, with the subject slightly facing right or left, was 8.93. The system scored seventy-four of the pictures less than the maximum score, which is ten, mostly because the pictures had focus and brightness problems. However, these problems did not prevent the system from recognizing and matching the pictures. Therefore, it is obvious that even though the pictures may have some technical problems, the face recognition systems are likely to work with lower quality images.

Table 2: Mean of Recognition Scores

	N	Minimum	Maximum	Mean
MUGSHOTS	**140**	**7.91**	**10.00**	**9.8380**

Table 3: Frequency of Recognition Scores
MUGSHOTS

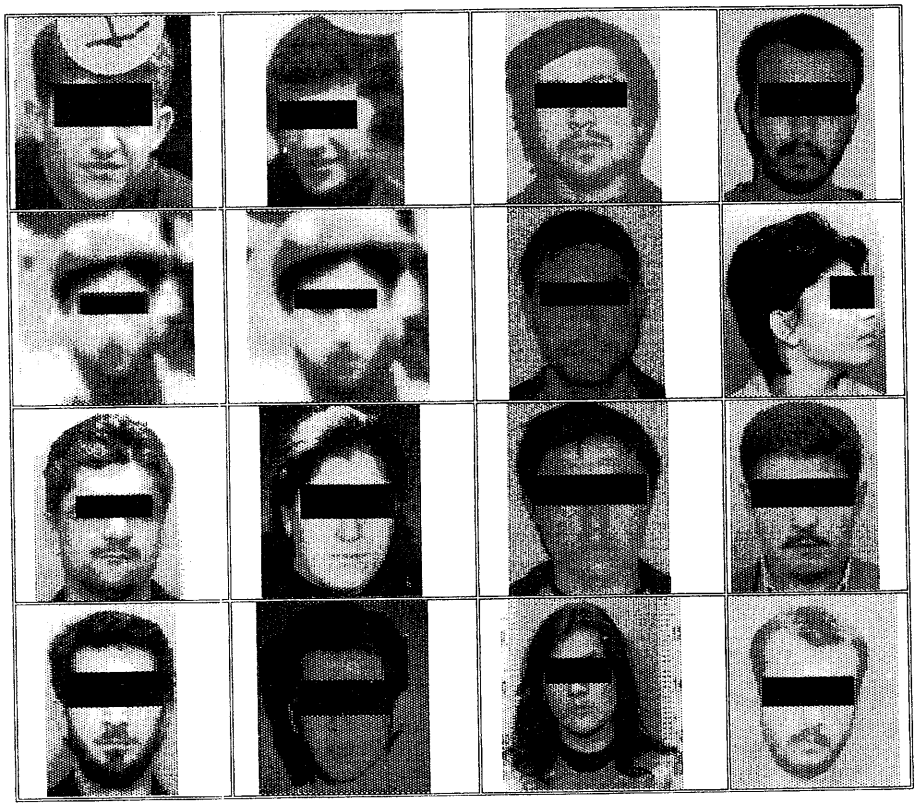
	Score	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	7.91	1	.7	.7	.7
	8.93	1	.7	.7	1.4
	9.07	1	.7	.7	2.1
	9.43	1	.7	.7	2.9
	9.45	1	.7	.7	3.6
	9.47	1	.7	.7	4.3
	9.50	1	.7	.7	5.0
	9.52	2	1.4	1.4	6.4
	9.54	1	.7	.7	7.1
	9.56	1	.7	.7	7.9
	9.59	1	.7	.7	8.6
	9.60	1	.7	.7	9.3
	9.62	1	.7	.7	10.0
	9.63	1	.7	.7	10.7
	9.64	1	.7	.7	11.4
	9.65	3	2.1	2.1	13.6
	9.66	1	.7	.7	14.3
	9.67	2	1.4	1.4	15.7
	9.68	2	1.4	1.4	17.1
	9.69	1	.7	.7	17.9
	9.70	1	.7	.7	18.6
	9.71	1	.7	.7	19.3
	9.72	4	2.9	2.9	22.1
	9.73	2	1.4	1.4	23.6
	9.74	3	2.1	2.1	25.7
	9.75	1	.7	.7	26.4
	9.76	2	1.4	1.4	27.9
	9.77	5	3.6	3.6	31.4
	9.78	6	4.3	4.3	35.7
	9.79	3	2.1	2.1	37.9
	9.80	1	.7	.7	38.6
	9.81	4	2.9	2.9	41.4
	9.82	2	1.4	1.4	42.9
	9.84	1	.7	.7	43.6
	9.85	1	.7	.7	44.3
	9.86	2	1.4	1.4	45.7
	9.88	2	1.4	1.4	47.1
	9.89	4	2.9	2.9	50.0
	9.94	2	1.4	1.4	51.4
	9.96	2	1.4	1.4	52.9
	9.99	1	.7	.7	53.6
	10.00	65	46.4	46.4	100.0
	Total	140	100.0	100.0	

Conclusion

It is obvious that face recognition is an emerging and fairly new technology. As we planned our projects based on face recognition systems, we weren't sure wHeather face recognition systems were reliable enough to be used for law enforcement. As we processed our images and loaded them into our system, we realized that face recognition technology is actually working because we received a one hundred percent positive recognition ratio for this dataset. Face recognition systems can be used by both law enforcement and private business in daily routine tasks. Consequently, we can use face recognition technology for both of the projects to find missing children and a nationwide implementation of face recognition-based investigation and security tools for law enforcement in Turkey.

Implications of new inventions may take some time. It is also obvious that because face recognition technology is an innovative application in biometrics, it still requires more enhancements to be more useful. There is a need for further research on face recognition. However, the more the face recognition systems are used the more improvements in the technology will be available.

SAMPLE PICTURES



Acknowledgements

The author thanks to Dr. Brian O'Connor for his contribution and comments, which facilitated to shape the article. The author is also grateful to Samih Teymur, İsmail Yılmaz and Murat Öztürk for their inspiration to the projects and their help in providing the images.

Bibliography

American Banker, (1999), "Italy Banks Using Face Recognition System," American Banker-Bond Buyer WELLESLEY, Mass volume 164, number 129, (8 July, 1999) pp. 14. at http://www.americanbanker.com, accessed 16 April 2003.

Bone, M, and C., Crumbacker, (2001), "Face Recognition Systems and Prison Access Control," *Corrections Today*, volume 63, number 4 (July 2001), pp. 62

Buckler,G., (1997), "West Virginia to Use Face Recognition for Licenses," Newsbytes, (10 September, 1997) pNEW09100027

Chien, Jen-Tzung and Chia-Chen Wu, (2002). "Discriminant Waveletfaces and Nearest Feature Classifiers for Face Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* volume 24, number 12 (December 2002), pp. 1644-1649.

Clark, L, (2002), "Florida Officials Considering Face Recognition, Fingerprinting Use with Driver Licenses," *Knight Ridder/Tribune News Service,* (8 January) 2002 pK7373

Delaney, D, (2002), "Thunder Bay International Airport the First Canadian Airport to Use," Pressbox.co.uk at http://www.pressbox.co.uk/Detailed/4699.html, accessed 16 April 2003.

DiDio, L, (1998), "These ATMs Never Forget a Face," *Computerworld,* volume 32, number 22 (1 June, 1998) pp. 33

Edwards, G.J.; C.J.Taylor and T.F.Cootes, (1997), "Learning To Identify and Track Faces in Image Sequence," at www.bmva.ac.uk/bmvc/1997/papers/104/paper.html, accessed 15 April 2003.

FBI-NCIC, (2003), "Federal Bureau if Investigation, National Crime Information Center (NCIC), Missing Person File," at www.fbi.gov, http://www.interpol.int/Public/Children/Missing/Default.asp

FERET, (2003), "Face Recognition Technology Program." at http://www.dodcounterdrug.com/facialrecognition/Feret/feret.htm accessed 15 April 2003.

Franceschina, P, (2002), "Palm Beach Airport Launching Face-Recognition System," *Knight Ridder/Tribune News Service,* (16 January, 2002) pp. K2224

Gao, Yongsheng and Maylor K.H. Leung, (2002), "Face Recognition Using Line Edge Map," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* volume 24, number 6 (June 2002), pp. 764-779.

Gips, M, A, (2002), "Face recognition Blasted again," *Security Management,* volume 46, number 8, (August 2002) pp. 18.

Harrison, C, (2002), "Face-Recognition Technology Will Screen Passengers at Dallas-Area Airport," *Knight Ridder/Tribune Business News,* (9 January, 2002), pp. ITEM02009041

Hindus, L, (2002), "Big Brother is Watching," *Advanced Imaging,* volume 16, number 4 (July 2001) pp. 62.

Hong, Lin and Anil Jain, (1998), "Integrating Faces and Fingerprints for Personal Identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* volume 20, number 12 (December 1998), pp 1295-1307.

Imagis Technology Inc. (2003), "Company Overview" at http://www.integratir.com/overview.asp?ticker=v.nab, accessed 15 April 2003. Also available through Market News Publishing, July 3, 2002 p1008184w1322.

Inminstry, (2003), "Statistics," at http://www.inministrytochildren.org/facts/stats.html, accessed 16 April 2003.

INS SENTRI, (2003), "Secure Electronic Network for Travelers Rapid Inspection," Immigration and Naturalization webpage at http://www.immigration.gov/graphics/shared/lawenfor/bmgmt/inspect/sentri.htm , accessed 15 April 2003.

Interpol, (2003), "Missing Children," at http://www.interpol.int/Public/Children/Missing/Default.asp. accessed 16 April 2003.

Jia, X. and M. S. Nixon, (1995), "Extending the Feature Vector for Automatic Face Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* volume 17, number 12 (December 1995), pp. 1167-1176.

Kelsey, D, (2001), "Colorado to Use Face Recognition Photos to Stop ID Theft," *Newsbytes*, (5 July, 2001) pNWSB01186002

Kerber, R, (2002), "Biometrics in Human Services" volume 6, number 2 (March 2002) at http://www.dss.state.ct.us/digital/news27/bhsug27.htm, accessed 15 April 2003.

Kirby, M, and L, Sirovich, (1990), "Application of the Karhunen-Loeve Procedure for the Characterization of Human Faces," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* volume 12, number 1 (January 1990), pp. 103-108.

Kohonen, T., (1988), *Self-organization and Associative Memory.* 2nd edition, Berlin New York: Springer-Verlag

Lyons, M. J.; J. Budynek and S. Akamatsu, (1999), "Automatic Classification of Images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, volume 21, number 12 (December 1999), pp. 1357-1362.

McGuire, D, (2002), "Virginia Beach Installs Face-Recognition Cameras," *Washington Post*, July 3 2002.

Mills, K, (2003), "Qantas Adopts Facial Scan Security," *Australasian Business Intelligence,* (4 October, 2002) pp. 1008277i7731

Pentland, A. and T. Choudhury, (2003), "Personalizing Smart Environments: Face Recognition for Human Interaction," at http://www-white.media.mit.edu/tech-reports/TR-516/, accessed 15 April 2003.

Rothstein, L, (2001), "Stop that Face!" *Bulletin of the Atomic Scientists*, volume 57, number 6 (Nov-Dec 2001) pp. 6-9.

Silva, S, D, (2002), "Totalitarianism with a Human Face: the Combination of Surveillance Cameras and Face-Recognition Software is Creating New Threats to Such Freedoms as Remain," *Arena Magazine*, {April-May 2002} pp. 17.

Stock, H, (2000), "Face-Recognition Check Cashers for Banks," *American Banker*, volume 165, number 100 (24 May, 2000) pp. 8

Sung, Kah-Kay and Tomaso Poggio, (1998), "Example-Based Learning for View-Based Human Face Detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* volume 20, number 1 (January 1998), pp. 39-51.

Telecomworldwire, (2002), "FaceIt face recognition system identifies wanted individual in UK town centre," Jan 14, 2002.

Turk, M, and A, Pentland, (1991), "Eigenfaces for Recognition," *Journal of Cognitive Neuroscience*, volume 3, number 1 (January 1991), pp. 71-86.

Viisage, Inc. (2002), "Manchester Airport to Implement Viisage Face Recognition Technology to Enhance Airport Security," at http://www.viisage.com/May%20%2016, %202002. htm, accessed 16 April 2003.

Washington Post (through newsbytes), (1998), "Polaroid & Visionics Tout Face Recognition To DMVs." April 16, 1998 pNEW04160043. COPYRIGHT 1998 Newsbytes News Network BOSTON

Yang, M D.; J. Kriegman and N. Ahuja, (2002), "Detecting Faces in Images: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, volume 24, number 1 (January 2002), pp. 34-58.