Facial Recognition: Limited Application in Safety and Security

Anthony Ronald Grue

STS.035

Introduction:

The field of biometrics is concerned with the statistical study of biological properties. Computers ever since their conception are used as a tool for the statistical analysis due to their processing speed and storage capacity. In addition through the field of artificial intelligence computers made a name for themselves as symbolic processors. Biometrics is concerned with large quantities of data which need to be handled and analyzed statistically but have symbolic and not numeric representations making it a prime candidate for computer application.

Facial recognition with its first research in computing occurring in the mid seventies belongs to the field of biometrics. The human face also presents an interesting problem for a computer in its vagueness and complexity. There is the general structure, the uniqueness of the details of the features, the shading of the skin, facial hair, and then added accessories such as sunglasses which propose widely varying situations which are not typically seen in other image processing and recognition applications.

Facial recognition has been around for a considerable amount of time in the form of a photo id which is fairly trusted in our society. Until now the processor deciding whether a person is the same as one in a photo has always been a human brain and never a computer. Computers introduced into this type of identification however will not simply server to replace humans but have broadened the impact of the field. No longer is it only feasible to compare a person to the card they are holding in front of them but with facial recognition on a computer you can compare a person to a database of images which you store, enabling you to identify a person you have never meet before or for you to look for 1000 people at once and find at least some of them.

This however has sparked an enormous controversy with discussions pertaining to the reliability of facial recognition systems and whether or not they constrict freedom since facial recognition, unlike many other biometric identification techniques, can be entirely passive. Despite promises of stronger security and a safer country in the age of terrorism the recent lab to real world transition of facial recognition has meet its critics.

I argue that facial recognition technology has matured allowing accurate identification of individuals wishing to be identified but that facial recognition is primarily being used in an attempt to solve safety and security problems which it can not hope to tackle and thus is bound to be ostracized by society for its great potential to invade an individual’s privacy.

Background:

Since the early 1950’s when digital computers were born and the world gained significant processing power, computer scientists have endeavored in bringing thought and the senses to the computer. Vision is a core element in the human experience and if computers gained the gift of sight they would be one large step closer to fully integrating into human society and could be capable of providing a vast majority of useful functions such as recognizing and classifying environments the computer interacts with or identifying people by their pictures in a large database.

The very first step towards machine vision was at the National Bureau of Standards on their SEAC computer. With recent developments in AI and the importance of symbolic processing coming to light Russell Kirsch made the move as the first to do image processing by designing a drum scanner which read in a small picture of his baby son and the executed algorithms to process the image cleaning it up for the computer and thus starting the field of image processing (pg. 9, Kirsch).

The next logical step towards making computers user friendly, intelligent, and humanlike would be their ability to recognize humans to eventually enable interaction. Facial recognition was picked up in the early seventies by M.D. Kelley and then Takeo Kanade as an interesting problem in machine vision. At first the focus in identifying faces was on patterns and particular facial features (pg. 470, Zhao). Over time emphasis has grown to building a set of faces which can be combined together to form any face, thus paying attention to the mathematical variations in peoples faces instead of their features.

With humans an inherent problem exists in that we can only know so many people because we can only sustain a social network of limited depth. Computers however are capped only in their storage space. This gives computers the potential to know everyone and interact with them or identify them. The technical challenge for computers is not remembering many faces but trying to differentiate people in a large database because the more individuals you have the less differentiated they will be.

While the technical challenge is slowly being overcome the even more difficult problem of social acceptance is being encountered. Plagued with the fears expressed in George Orwell's 1984 most members of society are very concerns about the use of a computer system which is capable of recognizing them wherever they go. If the system succeeds in its task it could then inform the government of anyone's whereabouts at any time and inventing big brother quite successfully. September 11th and the rise of terrorism awareness has given the government an window of opportunity in which Americans are willing to give up some privacy, freedom, and convenience in order to be better protected and some have used this window to try facial recognition in public places.

Technical Material Overview:

Takeo Kanade in his 1977 thesis *Computer recognition of human faces* presents the first work in facial recognition. Facial recognition like many other fields, such as speech recognition, was a process that was not understood when it was first attempted on a computer. Thus Kanade spent effort postulating how a human looks at another individuals face and is immediately able to recognize that it is indeed a human face and identify all the features and where they are located on the face. Most importantly if they have seen the person before they recognize the face and can correctly associate it with that person's identity. Due to interest from the image recognition community and interests in application by the government and commercial communities' facial recognition provided itself as a reasonable problem to tackle on a computer so he made the first attempt (pg. 1, Kanade).

The image recognition and artificial intelligence community saw facial recognition as a problem of symbolic recognition paralleling problems of text recognition which at the time was a recent success in the community. Two glaring differences however, stood out. The first was the range of quality that different pictures can have. The differences in two pictures of the same person due to poor camera, improper lighting, and other photographic aspects must first be eliminated in order to further analyze the image. The second difference from standard symbolic recognition is that unlike text there is no predefined pattern of exclusive objects at fairly fixed distances. To cope with these issues any system that was to be designed had to be extremely flexible and determine on the fly which parts of a picture are relevant to facial recognition and then further analyze those parts.

While Kanade's system was surprisingly successful at classifying pictures it still had a fair share of problems which included failing even classifying of all faces which had a beard and 63 of 79 test cases where the face had any turn or tilt. Out of these 800 faces used however, 40 where chosen for recognition tests and where correctly identified 45-75% correct identification. One interesting point Kanade made was by having a human perform the algorithm by hand which provided a 75% success rate. While it took longer the human actually turned out more accurate at the algorithm. This demonstrated that computers could still make significant increases in reliability as the field matured.

Since Kanade's work much progress has been made the biggest technically is in the shift to the eigenfaces method What started as a interesting way to model surfaces which fluids would flow over this DARPA funded research evolved into a way to store facial images using a small set of core data (pg. 3, Wisniewski). This method creates a library of eigenfaces, a set of images ranging in quantities of 8 to 100 in which all stored faces are a linear combination of. This method heavily relies on preprocessing making the face the right angle with the right lighting before encoding as a linear combination of the eigenfaces in the system. The primary advantage to this system is it allows very rapid searching for a match because once you have encoded a face in eigenface you can look to see if there is another one in your database that is very similar.

Introduction to Society:

Research having begun 25 years ago facial recognition products are starting to emerge into real life application and have brought the US population to their attention particularly since the rising threat of terrorism. In 2001 the city of Tampa, Florida monitored every attendant of the Super Bowl using FaceIt the most prominent facial recognition application on the market, created by Visionics Corporation. No suspects were identified however despite the attendance of 71,000 people (Woodward). In addition Tampa, a few other cities, and some airports including Boston's Logan have installed face recognition software which to date has been ineffective at identifying any criminal suspects (Bray).

Some police agencies however, have been using more benevolent forms of facial recognition. When presented with an image of a suspect they can enter the image into a computer that then presents them with a list of possible matches of people who already have a criminal record. None of which are guaranteed to be the suspect but it gives law enforcement a starting point and allows them to take more information into consideration though further investigation than just the persons facial identity as determined by the computer.

Analysis of the Success and Need of Facial Recognition:

First I believe computers are capable of facial recognition and in a way that parallels the way humans perform the task. Kanade's technique takes localized features on the face and deeply analyzes them for shapes, designs and certain measurement values and then compares those against others in a database. The eigenface technique using different maps which contain all the features of human faces a key is build containing the linear combination of the maps needed to reproduce the face using this key for easy comparison and look up. These strategies are each a piece of how a human being recognizes a face. We use a "holistic" approach in which we consider both the general structure and differences but also record in our mind precise information about the other persons features (pg. 411, Zhao). To demonstrate the capabilities of facial recognition systems a standard database and method for testing these systems, FERET was developed to ensure levels of reliability. FERET is a database and testing standard that includes a library of images and procedures for the tests (pg. 61, Phillips). The conception of FERET demonstrates that people expect accountability from facial recognition software.

The most important issue in facial recognition which the engineers have some control over is whether or not computers can be trusted to the task. The first issue to be considered for any system when considering trustworthiness is what the system is going to be used for and whether or not it satisfies the requirements of the situation. As in any system the more accurate facial recognition is the more trusted it will be but the way it is used is even more important. Facial recognition can be used in two manners one is to identify a person by using a database of previously acquired pictures the other is to verify a person is who they claim they are (pg. 56, Phillips). Facial recognition allows for thresholds of detection which adjust how close a face must be to one in the database to make a positive match. For identification purposes the system should have a very low tolerance thus preventing the likelihood of false identifications of the wrong individual. However in cases where facial recognition is used to confirm you are who you claim you are tolerance can vary more greatly. If you wish not to present an inconvenience you would set a fairly loose threshold but if you didn't want any false verification you would set it high in realization that some legitimate matches would be lost (pg. 57, Phillips). As a result of the flexibility of the sensitivity you can build a fairly trustworthy system if the application is considered.

Humans however, tend to set their standards for computer reliability far greater than standards for themselves or other human beings. When a human makes a mistake we are sympathetic and understanding because we have shared the experience When a computer makes a mistake though we tend to believe that the fault is inherit in the system and will repeat itself, thus believing any fault no matter the size indicates a fundamental flaw in the system. Statistically though facial recognition technology does a surprising job at accurately identifying individuals and not making very many false positives. In face recognition tests for verification on FERET between 1994 and 1996 the false verification rates over different days was two percent and over 1.5 years was still 2 percent(pg. 61, Phillips). A false negative was 11 percent on different days and 43 percent over 1.5 years. Legally one of the most accepted forms of evidence in a police station or a court is an eyewitness. People trust that they are capable of recognizing others however in a study of lineup procedures it was recorded that in lineups of six to eight people that are absent of the perpetrator a witness will misidentify an individual 43% of the time due to the biases they have and the belief that one of the six or eight must be the one they are looking for. In addition humans judge the members of a line up against each other and build up evidence in their mind that one of the line members must be the perpetrator because they look the same in comparison to the rest of the line (pg. 2, Steblay). Computers do not have the human biases built in to them and thus turn out to be more effective at protecting the innocent by not falsely identifying an individual as a suspect. Despite this incredible demonstration computers remain with a lack of human trust. To gain the trust of the population system designers will have to further invest in tests like FERET that convinces people of the technologies power.

If we don't trust computers why spend time, money, and effort in the development and deployment of facial recognition technology. The reason is a desire by the general population for more regulated and secure environments. The government is interested in the technology to fight general crime and in the post September 11th world because the public is asking the government why they failed in preventing the attack. The government as a result is turning to look for a technological fix for a serious problem one that can not be fully rectified through monitoring the entire American population with facial recognition systems. DARPA none-the-less started its Human ID at a Distance program funding which provided a grant to Visionics among other companies to continue their research (Woodward). DARPA is looking for technology that can identify people in crowds and at long ranges which they believe would permit them to better identify suspects in the field off United States soil and in the US. The essence of a need to better track people from an intelligence point of view is revealed. If it was possible to know where everyone was at anytime then if ever an individual was a danger to society they would be able to be stopped. In this seemingly perfect world however there would be no freedom and thus the idea of safety becomes a far less valuable goal.

Facial recognition allows us to evaluate its success in two lights due to its having existed in the lab and it having been introduced into people's lives. The first is from a technical standpoint which as demonstrated by the FERET tests it is becoming increasingly successful in. The second however is whether or not it achieves the goal of providing better security and saftey in environments where it is deployed. Boston's

Logan Airport has adopted the technology in light of the September 11th attacks and is spending a considerable amount of time testing the system and trying employs in its use (Bray). However at the time of the September 11th attacks, only 2 of the 19 terrorists were even know to United States and for only one did a picture exist (ACLU). The facial recognition system would not have come through had it been implemented then, not because the technology was lacking, but because the human factor of identifying which people in the population are terrorists and not ordinary residents.

Additionally, the facial recognition software is easily fooled by those looking into the camera at different angles and those with sunglass or a beard. As a result facial recognition is only reliable when the subject is wishing to be identified. If they are trying to hide on the other hand there are fairly cheap solutions to an expensive to implement solution just grow facial hair or wear sunglasses and you have rendered all current techniques of facial recognition useless. Returning to understanding the purpose of your system, for Logan to achieve its goal of eliminating terrorists on planes with facial recognition technology they would have to have a list of all approved passengers and a low tolerance in their system. This would create such a large inconvenience to the flying public however that it is a useless solution.

Conclusion:

Facial recognition has meet considerable success in achieving the ability to verify identities in certain environments using both facial features and eigenfaces but that is not enough to make the technology a success. Unfortunately it attempts to solve the problems of crime and poor security by using a identification system that everyone is already inducted into. Unfortunately this system does not bring about an increase in security since it is so easily stepped around. Facial recognition technology has its uses but can only expand so much. Used by police departments facial recognition can provide investigators a way to make a hunt for perpetrators more efficient, but not entirely replace the hunt. Like machine translation for the government, facial recognition too is best used when it assists people by narrowing down the field of data which they are exposed to instead of trying to evaluate it all my itself. In addition it leaves human beings in the loop and is only used when necessary.

Capturing images of everyone in their day to day tasks merely strips them of all privacy they have and indeed realizes the big brother society that the public is rightly afraid of. Safety and national security are important goals but not at the cost of our freedoms and using facial recognition this will do little but scar it. It is clear that facial recognition technology has great potential in the verification of identities. It's use however must be closely monitored and can not be applied to fix problems when external factors prevent it from any possible success.

Works Citied:

Primary Sources:

Kirsch, Russell. SEAC and the Start of Image Processing at the National Bureau of Standards. IEEE Annals of the History of Computing, Vol. 20, No. 2, 1998

Kanade, Takeo. Computer recognition of human faces. 1977.

Wisniewski, Helena. Face Recognition and Intelligent Software Agents – An Integrated Ssytem. Prepared for the U.S. Senate Committee on Commerce, Science, and Transportation.

Secondary Sources:

Phillips, P. Jonathon. Martin, Alvin. Wilson, C.l. Przybocki, Mark. An Introduction to Evaluating Biometric Systems. National Institute of Standards and Technology. Computer. IEEE. Vol. 33, No. 2, February 2000

W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld. 2003. **“**Face recognition: A literature survey.” ACM Computing Surveys (CSUR). ACM Press New York, NY.

“Q&A On Face-Recognition.” ACLU Privacy & Technology: Surveillance & Wiretapping. September 2, 2003.

Bray, Hiawatha. Reliability of face scan technology in dispute. *Boston Globe*, August 5, 2002.

Woodward, John D. Super Bowl Surveillance: Facing Up to Biometrics. RAND Documents. 2001.

Sources for External Information:

Nancy Steblay, Jennifer Dysart, Solomon Fulero, and R. C. L. Lindsay. Eyewitness Accuracy Rates in Sequential and Simultaneous Lineup Presentations: A Meta-Analytic Comparison. Law and Human Behavior, Vol. 25, No. 5, October 2001.