A

Seminar report

On

Face Recognition Technology

Submitted in partial fulfillment of the requirement for the award of degree
Of ECE

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Preface

I have made this report file on the topic Face Recognition Technology**;** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the prepration of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Abstract

A face recognition technology is used to automatically identify a person through a digital image. It is mainly used in security systems. The face recognition will directly capture information about the shapes of faces. The main advantage of facial recognition is it identifies each individual's skin tone of a human face's surface, like the curves of the eye hole, nose, and chin, etc. this technology may also be used in very dark condition. It can view the face in different angles to identify.

It is mainly used in airports were it ill recognize the face and we can avoid some unwanted terrorist. When compared with other biometrics systems using fingerprint and iris, face recognition has different advantages because it is without touching the person. Trough Face images we can capture the person identification from a distance without touching or interacting with them. And also face recognition is used for crime restriction purpose because face images that have been recorded and archived, so that it ill help us to identify a person later.

This report develops a socio-political analysis that bridges the technical and social-scientific literatures on FRT and addresses the unique challenges and concerns that attend its development, evaluation, and specific operational uses, contexts, and goals. It highlights the potential and limitations of the technology, noting those tasks for which it seems ready for deployment, those areas where performance obstacles may be overcome by future technological developments or sound operating procedures, and still other issues which appear intractable. Its concern
with efficacy extends to ethical considerations

Introduction

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication.

Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearences. Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes.

Despite warning, many people continue to choose easily guessed PINâ„¢s and passwords: birthdays, phone numbers and social security numbers. Recent cases of identity theft have highten the need for methods to prove that someone is truly who he/she claims to be

Face recognition technology may solve this problem since a face is undeniably connected to its owner expect in the case of identical twins. Its nontransferable. The system can then compare scans to records stored in a central or local database or even on a smart card.

What is Face Recognition?

Face recognition technology is the least intrusive and fastest biometric technology. It works with the most obvious individual identifier – the human face.

Instead of requiring people to place their hand on a reader(a process not acceptable in some cultures as well as being a source of illness transfer) or precisely position their eye in front of a scanner, face recognition systems unobtrusively take pictures of people's faces as they enter a defined area. There is no intrusion or delay, and in most cases the subjects are entirely unaware of the process. They do not feel "under surveillance" or that their privacy has been invaded.

History of Face Recognition

The subject of face recognition is as old as computer vision, both because of the practical importance of the topic and theoretical interest from cognitive scientists. Despite the fact that other methods of identification (such as fingerprints, or iris scans) can be more accurate, face recognition has always remains a major focus of research because of its non-invasive nature and because it is people's primary method of person identification.

Perhaps the most famous early example of a face recognition system is due to Kohonen , who demonstrated that a simple neural net could perform face recognition for aligned and normalized face images. The type of network he employed computed a face description by approximating the eigenvectors of the face image's autocorrelation matrix; these eigenvectors are now known as `eigenfaces.'

Kohonen's system was not a practical success, however, because of the need for precise alignment and normalization. In following years many researchers tried face recognition schemes based on edges, inter-feature distances, and other neural net approaches. While several were successful on small databases of aligned images, none successfully addressed the more realistic problem of large databases where the location and scale of the face is unknown.

Kirby and Sirovich (1989) later introduced an algebraic manipulation which made it easy to directly calculate the eigenfaces, and showed that fewer than 100 were required to accurately code carefully aligned and normalized face images. Turk and Pentland (1991) then demonstrated that the residual error when coding using the eigenfaces could be used both to detect faces in cluttered natural imagery, and to determine the precise location and scale of faces in an image.

They then demonstrated that by coupling this method for detecting and localizing faces with the eigenface recognition method, one could achieve reliable, real-time recognition of faces in a minimally constrained environment. This demonstration that simple, real-time pattern recognition techniques could be combined to create a useful system sparked an explosion of interest in the topic of face recognition.

How Facial Recognition Systems Work

Anyone who has seen the TV show "Las Vegas" has seen **facial recognition software** in action. In any given episode, the security department at the fictional Montecito Hotel and Casino uses its video surveillance system to pull an image of a card counter, thief or blacklisted individual.

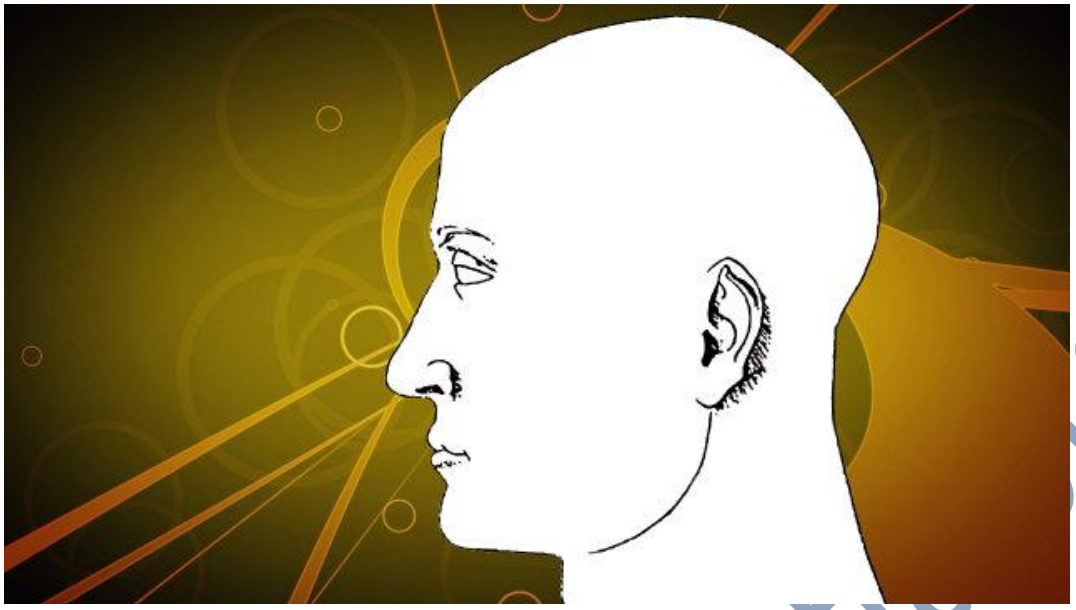
It then runs that image through the database to find a match and identify the person. By the end of the hour, all bad guys are escorted from the casino or thrown in jail. But what looks so easy on TV doesn't always translate as well in the real world.

In 2001, the Tampa Police Department installed police cameras equipped with facial recognition technology in their Ybor City nightlife district in an attempt to cut down on crime in the area. The system failed to do the job, and it was scrapped in 2003 due to ineffectiveness. People in the area were seen wearing masks and making obscene gestures, prohibiting the cameras from getting a clear enough shot to identify anyone.

Boston's Logan Airport also ran two separate tests of facial recognition systems at its security checkpoints using volunteers. Over a three month period, the results were disappointing. According to the Electronic Privacy Information Center, the system only had a 61.4 percent accuracy rate, leading airport officials to pursue other security options.

Humans have always had the innate ability to recognize and distinguish between faces, yet computers only recently have shown the same ability. In the mid 1960s, scientists began work on using the computer to recognize human faces. Since then, facial recognition software has come a long way.

In this article, we will look at the history of facial recognition systems, the changes that are being made to enhance their capabilities and how governments and private companies use (or plan to use) them.



Applications of face recognition system

1. **Law enforcement and justice solutions:**

• Today's law enforcement agencies are looking for innovative technologies to help them stay one step ahead of the world's ever-advancing criminals.

• As such, FRS is committed to developing technologies that can make the jobs of the law enforcement officer easier. This includes acclaimed CABS-computerized arrest and booking system and the childbase protection, a software solution for global law enforcement agencies to help protect and recover missing and sexually exploited children, particularly as it relates to child pornography.

CABS:

• Store all offence-related detain one easy-to-use system -- data is entered once and only once.

• Integrate with any database -- including other detachments and other applications (RMS, CAD, Jail Management systems, and "most-wanted" databases) .

• Link victims to offenders -- to aid in criminal analysis and investigations

• Capture and store digital images of the offender -- encode all mug shots, marks, tattoos, and scars

• Perform rapid and accurate searches -- on all data and image fields for crime statistics and reporting

• Produce digital lineups -- using any stored image in minutes

• Identify previous offenders -- pre-integrated with advanced biometric face recognition software.

Childbase protection:

• ChildBase is an application that helps protect and recover missing and sexually-exploited children, particularly those children victimized through child abuse images.

2 Identification solutions:

With regards to primary identification documents, (Passports, Driver's licenses, and ID Cards), the use of face recognition for identification programs has several advantages over other biometric technologies.

• Leverage your existing identification infrastructure. This includes, using existing photo databases and the existing enrollment technology (e.g. cameras and capture stations); and

• Increase the public's cooperation by using a process (taking a picture of one's face) that is already accepted and expected;

• Integrate with terrorist watch lists, including regional, national, and international "most-wanted" databases.

3 Homeland defence:

• Since the terrorist events of September 11, 2001, the world has paid much more attention to the idea of Homeland Defense, and both governments and private industries alike are committed to the cause of national defense.

• This includes everything from preventing terrorists from boarding aircraft, to protecting critical infrastructure from attack or tampering (e.g. dams, bridges, water resevoirs, energy plants, etc.), to the identification of known terrorists.

4 Airport security:

• Airport and other transportation terminal security is not a new thing. People have long had to pass through metal detectors before they boarded a plane, been subject to questioning by security personnel, and restricted from entering "secure" areas. What has changed, is the vigilance in which these security efforts are being applied.

• The use of biometric identification, can enhance security efforts already underway at most airports and other major transportation hubs (seaports, train stations, etc.).

• This includes the identification of known terrorists before they get onto an airplane or into a secure location.

5 Immigration:

• Most countries do not want to be perceived as being a "weak link" when it comes to accepting immigrants and refugees, particularly if that individual uses the new country as a staging ground for multi-national criminal and terrorist activities. Consequently, governments around the world are examining their immigration policies and procedures.

• Biometric technology, particularly face recognition software, can enhance the effectiveness of immigration and customs personnel. After all, to the human eye it is often difficult to determine a person's identity by looking at a photo, especially if the person has aged, is of a different ethnic background, has altered their hair style, shaved their beard, etc. FRS does not have this difficulty.

6 Access control:

• The use of biometric technology, particularly face recognition software (either independently or as one part of a multi-layered biometric solution), can enhance your security efforts considerably.

• Biometric identification ensures that a person is who they claim to be, eliminating any worry of someone using illicitly obtained keys or access cards.

7 Financial services:

• The financial services industry revolves around the concept of security. Yet for the most part, security within the industry is limited to a simple personal identification number (PIN) or password.

• Biometrics, particularly face recognition software, can improve the security of the financial services industry, saving the institution time and money both through a reduction of fraud cases and the administration expenses of dealing with forgotten passwords.

• Furthermore, biometric-based access control units can safeguard vaults, teller areas, and safety deposit boxes to protect against theft.

• The use of biometrics can also ensure that confidential information remains confidential while deterring identity theft, particularly as it relates to ATM terminals and card-not-present e-commerce transactions.

8 **Scene analysis and surveillance solutions:**

• This includes the ability to extract, categorize, and search non-facial imagery. For example, within the law enforcement application it allows you to capture, archive, and retrieve such identifying characteristics as tattoos, marks, or scars.

• It can also analyse scenes from either streaming or archived video, "looking" for out-of-the-ordinary occurrences, the presence of certain vehicles, specific faces, etc.

• This is beneficial and can save significant time and money to those individuals who spend hours, days, or weeks monitoring video streams (i.e. examining a bank's security in a criminal investigation).

How is facial recognition being used today?

Facial recognition is alive and flourishing. It's used in many broad areas, including social networking, photo editing, security, law enforcement, casinos, and in odd places that you might not expect. For example, the dating website FindYourFaceMate.com based matchmaking around the principle that people with similar facial features are attracted to each other, using facial recognition to match user photos, and DoggelGanger.com matches potential dog owners with canines that look like them.

Face recognition cameras scanned all the fans walking through the turnstiles at Super Bowl XXXV, now referred to as the Snooper Bowl, running the scans against a database of criminal mugshots. That was a decade ago, when the internet was still in its relative childhood. We're in an age now when Facebook collects 100-page dossiers on all of us, when ad networks track everything we do online, when companies buy and sell our contact information: the street we grew up on, the names of our family members, aerial shots of our homes.

SceneTap's interface. The app lets you check the gender ratio of a bar before you head over.

Lots of mobile apps use facial recognition, too. A particularly interesting one, Scene Tap, tracks the ratios of males to females and ages at 250 participating U.S. bars. These bars install face-

detection cameras, and the app calculates the number of people at the bar, the male-to-female ratio, and the average age of patrons. SceneTap doesn't receive bar patrons' permission to capture their faces and share demographic information about them. Another notable app is FACER Celebrity, made by Animetrics Inc., a facial-recognition company based in Conway, N.H., that focuses on the law-enforcement and security industries. FACER Celebrity is a free iPhone app that allows users to match their face to a star. The app, which has about 30,000 downloads, uses the same facial-recognition technology deployed by local law enforcement to identify criminal suspects, says Animetrics CEO Paul Schuepp.

Companies give two main reasons for using facial recognition technology: it helps with security, and it makes photo editing and sharing easier. On the security side, law enforcement officials have argued that facial recognition can help find missing people, identify criminals in a crowd, preempt terrorists from boarding planes with fake passports. It's also used for private security in casinos to identify card counters and kick them out before they can win too much. Casinos also say their systems identify people with gambling addictions who've asked casinos to forcibly remove them if they can't stop themselves. Even supermarket security uses facial recognition: one grocery chain in the UK uses facial recognition to stop underage customers from buying alcohol.

On the photo sharing side, facial recognition can scan albums for faces and either suggest tags or automatically tag people. You'll already find it in Apple's iPhoto, Google's Picasaweb, Microsoft's Windows Live Photo Gallery, and other photo editors. It also collects information on different people's faces through existing tags: the more tags, angles, lighting types, hairstyles, and other details in your photos, the better the software's ability to pick you out in other photos. It's one thing to confine this technology to the photos on your own computer, but things get more complicated when the internet gets involved.

Facebook got in trouble with privacy advocates when it rolled out facial recognition by default. It's since dialed it back to "Tag Suggestions," which you can choose to disable. Even if you disable it, though, Facebook still collects information about your face whenever it's tagged. And when you consider that Facebook's 600 million members upload over 250 million photos every day, you see that they're building an empire of facial data. Rumor has it they're building a way to search for people by picture alone. And Google's Goggles app can already identify inanimate objects through photographs. Add already-existing facial recognition software to that, and you could "identify strangers on the street."

Limitations of Facial Recognition Technology

The Boston Marathon bombings revealed the limitations of facial-recognition technology to the general public. Many private citizens, accustomed to seeing computers on television and in the movies match photographs to motor vehicle and other databases in mere seconds, were surprised that our nation's premier law enforcement agencies did not have the same level of technological sophistication available to them when Boston's, and perhaps the country's, security had been threatened.

Since 9/11, the federal government has spent a great deal of money on facial-recognition technology, with grants in the millions of dollars going to state and local governments for database creation. Even though government databases contained pictures of both of the Boston suspects, technology could not match surveillance footage to database images.

Before addressing the limitations of today's technology, let's discuss how one type of facial-recognition technology works.

Face detection occurs first. The algorithms typically cycle through various boxes, looking for faces with a certain dimension. Inside those boxes, the system detects facial landmarks and assigns a score, providing a confidence level regarding whether the image is a face. Once confirmed as a face, the technology creates a template, generally based on factors such as the relative distance between the eyes, the spot just under nose and above the lip, and ear to ear.

The mathematical representation developed is then compared to other detected faces. The similarity in ratios between distances on various points of the face, typically focused around anchors, such as the nose, the eyes, the ears and the mouth, yields a score on a logarithmic scale. Close matches range from 3 to 5, and definite nonmatches are less than 1. When the same image serves as both probe and target, a score of 40+ is possible.

Several factors limit the effectiveness of facial-recognition technology:

1. Image quality

Image quality affects how well facial-recognition algorithms work. The image quality of scanning video is quite low compared with that of a digital camera. Even high-definition video is, at best, 1080p (progressive scan); usually, it is 720p. These values are equivalent to about 2MP and 0.9MP, respectively, while an inexpensive digital camera attains 15MP. The difference is quite noticeable.

2. Image size

When a face-detection algorithm finds a face in an image or in a still from a video capture, the relative size of that face compared with the enrolled image size affects how well the face will be recognized. An already small image size, coupled with a target distant from the camera, means that the detected face is only 100 to 200 pixels on a side. Further, having to scan an image for

varying face sizes is a processor-intensive activity. Most algorithms allow specification of a face-size range to help eliminate false positives on detection and speed up image processing.

3. Face angle

The relative angle of the target's face influences the recognition score profoundly. When a face is enrolled in the recognition software, usually multiple angles are used (profile, frontal and 45-degree are common). Anything less than a frontal view affects the algorithm's capability to generate a template for the face. The more direct the image (both enrolled and probe image) and the higher its resolution, the higher the score of any resulting matches.

4. Processing and storage

Even though high-definition video is quite low in resolution when compared with digital camera images, it still occupies significant amounts of disk space. Processing every frame of video is an enormous undertaking, so usually only a fraction (10 percent to 25 percent) is actually run through a recognition system. To minimize total processing time, agencies can use clusters of computers. However, adding computers involves considerable data transfer over a network, which can be bound by input-output restrictions, further limiting processing speed.

Ironically, humans are vastly superior to technology when it comes to facial recognition. But humans can only look for a few individuals at a time when watching a source video. A computer can compare many individuals against a database of thousands.

As technology improves, higher-definition cameras will become available. Computer networks will be able to move more data, and processors will work faster. Facial-recognition algorithms will be better able to pick out faces from an image and recognize them in a database of enrolled individuals. The simple mechanisms that defeat today's algorithms, such as obscuring parts of the face with sunglasses and masks or changing one's hairstyle, will be easily overcome.

An immediate way to overcome many of these limitations is to change how images are captured. Using checkpoints, for example, requires subjects to line up and funnel through a single point. Cameras can then focus on each person closely, yielding far more useful frontal, higher-resolution probe images. However, wide-scale implementation increases the number of cameras required.

Evolving biometrics applications are promising. They include not only facial recognition but also gestures, expressions, gait and vascular patterns, as well as iris, retina, palm print, ear print, voice recognition and scent signatures. A combination of modalities is superior because it improves a system's capacity to produce results with a higher degree of confidence. Associated efforts focus on improving capabilities to collect information from a distance where the target is passive and often unknowing.

Clearly, privacy concerns surround this technology and its use. Finding a balance between national security and individuals' privacy rights will be the subject of increasing discussion, especially as technology progresses.

Advantages and Disadvantages

Facial recognition technology is a fairly new way of identify people who could be dangerous or need to be located. It works by picking faces out of a crowd, obtaining the measurements necessary and comparing it to the images already in it's database.

Advantages:

- Can prevent card counters, etc. from entering casinos
-Can identify terrorists, criminals, etc.
-Can find missing children
-Prevents voter fraud
-Targets shoppers

Disadvantages:

-Isn't always accurate
-Hindered by glasses, masks, long hair etc.
-Must ask users to have a neutral face when pictures are being taken
-Considered an invasion of privacy to be watched

References

- www.google.com
- www.wikipedia.com
- www.studymafia.org