# TECHNIQUES OF DETECTION

Project Report Submitted in partial fulfilment of the Degree of

Bachelor of Technology in

Electronics and Communication Engineering

Under the supervision of
Ms. Pragya Gupta

Submitted By:
Karamvir Singh (091065)
Sahib Sethi(091080)
Chandra Harsha(091125)

To

विद्या तत्व ज्योतिसम:

JAYPEE UNIVERSITY OF
INFORMATION TECHNOLOGY

Jaypee University of Information Technology

Waknaghat, Solan – 173234, Himachal Pradesh

# CERTIFICATE

This is to certify that the work titled "**Techniques of Detection**" submitted by "**Karamvir Singh**" "**Sahib Sethi**" **and** "**Chandra Harsha**" in partial fulfilment for the award of degree of "**Bachelor of Technology**" of Jaypee University of Information Technology, Waknaghat has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor ……P Gupta 29/05/2013……

Name of Supervisor ……Ms. Pragya Gupta……

Designation ……Senior lecturer ~~Ms. Pragya Gupt~~……

Date ……29/05/13……

# ACKNOWLEDGEMENT

We take this opportunity to express our profound gratitude and deep regards to our guide **"Ms. Pragya Gupta, Sr. Lecturer"** for her exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by her time to time shall carry us a long way in the journey of life on which I am about to embark.

We are obliged to staff members of Jaypee University of Information Technology, for the valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of my assignment.

Signature of the student ........Karamvir........

Name of Student ...Karamvir Singh...

Date ...29/5/13...

Signature of the student ...Sahib Sethi...

Name of Student ...Sahib Sethi...

Date ......29/5/13....

Signature of the student ...Harsha...

Name of Student ...Ootla Chandraharsha

Date ...29/5/13...

# TABLE OF CONTENTS

# ABSTRACT

The objective was to design and implement various techniques of detection in MATLAB that will detect human parts in an image.

The problem of detection has been studied extensively. However, it is difficult to design algorithms that work for all illuminations, face colours, sizes and geometries, and image backgrounds. As a result, face detection remains as much an art as science.

Our method uses rejection based classification for face detection. The face detector consists of a set of weak classifiers that sequentially reject non-face regions. First, the non-skin colour regions are rejected using colour segmentation. A set of morphological operations are then applied to filter the clutter resulting from the previous step. The remaining connected regions are then classified based on their geometry and the number of holes. Finally, template matching is used to detect zero or more faces in each connected region.

A similar type of code was also developed which detect the human iris of an eye.

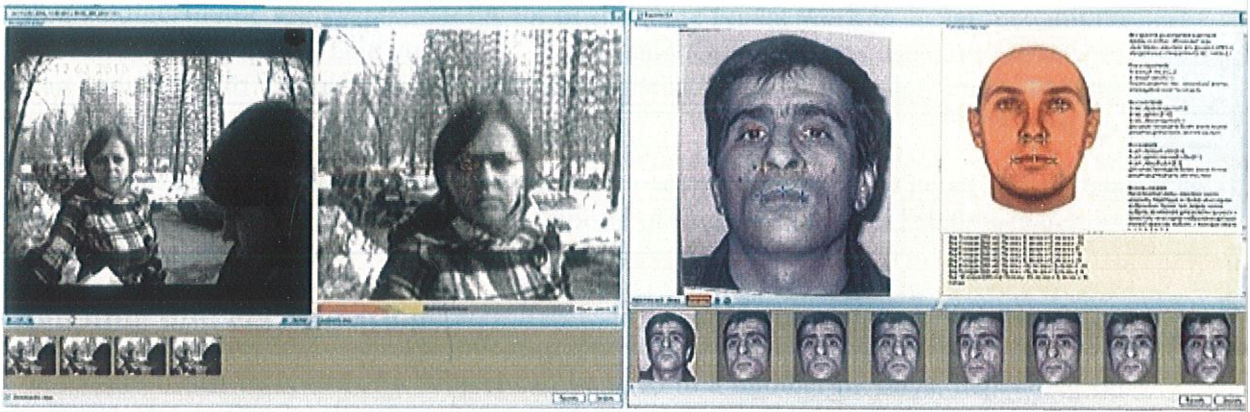
## Three steps to (sometimes) finding the perfect match

Under the best circumstances, facial recognition can be extremely accurate, returning the right person as a potential match more than 99 percent of the time with ideal conditions. But to get that level of accuracy almost always requires some skilled guidance from humans, plus some up-front work to get a good image. Depending on the type of facial recognition system, finding the right match usually requires three stages of processing.

### Face detection and enhancement

The software looks for patterns in the image that match models in its algorithms for faces. A simpler form of this technology is used in consumer cameras, in photo apps for mobile devices, and in entities like iPhoto or Facebook.

In some circumstances, even detecting a face within an image can be difficult for software without human guidance. Lighting, camera angle, and facial expression can all muddle the process. A photo will often be taken from an angle that requires investigators to do pre-processing. "Typically, you'll do some pre-processing of the image," said Brian Martin, director of Biometric Research for facial recognition system provider MorphoTrust USA. "You can try to get rid of blur or the interlacing artifacts from older cameras. Some people use Photoshop to clean up the image; our company has what we call ABIS Face Examiner Workstation, which is face-specific tools to clean up an image. You can take a non-frontal looking face and physically model it as a three-dimensional image, then rotate it toward the camera and re-render a new face. So you do this sort of cleanup of the image and then submit it to the database."



At left, a face from an ATM camera video is recognized and evaluated for facial recognition quality; at right, a photo of a face is enhanced with a 3D model to improve its searchability.

If an image is too low-resolution, sometimes multiple images can be combined to create a higher-resolution composite. Lower resolution images may still work, but the results are more likely to misidentify the person—or miss him or her completely.

"Hollywood does a pretty good job of creating a myth that you could extract a better image by enhancing and zooming where information wasn't captured," said Masayuki Karahashi, senior vice president of engineering for surveillance and video analysis technology firm 3VR. "You're not going to create more information out of nothing.

## Feature registration and extraction

Next, the software tries to identify common facial features to use as reference points to extract a "faceprint"—the centers of the eyes, tip of nose, and corners of the mouth are common features used for this. Again, depending on the quality of the image, a human may have to help the software with this, marking the location of reference points to help the software along.

With the reference points set, the software then adjusts the image to "normalize" it against the images in its database—making sure the face is scaled to the same size and removing other elements of the photo that might reduce the likelihood of a match. Then it runs calculations on the image to generate a faceprint. This is a binary value based on a mathematical representation of the patterns in the face.

There are several approaches to creating a faceprint. Some systems use algorithms that measure the distance between sets of features in the normalized image, while others detect contours and "facial boundaries."

Feature extraction is "the classic way" to gather data for facial recognition, according to Parham Aarabi, a professor of computer science at the University of Toronto and CEO of facial software firm ModiFace. "Another way is to do a direct match," he noted. This technique involves using the facial image itself as the basis of comparison rather than using an algorithmic representation. "A lot of the more recent work in facial recognition has been in direct face-to-face matching," Aarabi said. Other systems use multiple images of an individual to "learn" their facial characteristics to build a model, much like the Faces feature in Apple's iPhoto.

But in all of these approaches, the more detailed a source image is, the better. More data to base the faceprint on means a higher likelihood of success in the next steps—matching and classification.

## Matching and classification

The feature-based faceprint of a subject can be used in a number of ways, depending on the facial recognition application. Some systems perform additional indexing based on the images to classify the subject for narrowing searches, processing the faceprint with algorithms that can estimate the age and gender of the subject. Other characteristics, such as skin tone and facial features, can be used to help index the image as well, allowing for searches to be narrowed by race, estimated weight, or hair color.

Classification can also be used with what Martin called "short-term biometrics"—things such as gait recognition, or clothing, or other identifying features (such as a black backpack). These all can help locate a subject within a set of images or video streams. This approach was used to find the Tsarnaev brothers in surveillance video and other images collected from multiple sources by law enforcement. Video analysis showed Dzhokhar walking quickly and calmly away from the site of the second bomb as the first exploded; characteristics such as the brothers' ball caps and backpacks were used to quickly identify the suspects by retailers. These businesses had surveillance systems from vendors such as 3VR that could recognize relevant footage in their systems to provide to law enforcement.

"The fact that they were able to start looking for a person with a white baseball cap, a black bag—they were able to use those as variables to pull up videos," said Masayuki Karahashi, 3VR's senior vice president of engineering. Several 3VR customers were able to automatically pull results from their systems to provide to law enforcement from terabytes of video footage from the day.

Finding the actual identity of someone in an image still requires a match against a facial database. In a facial recognition search, the binary faceprint of the subject is checked against those of a collection of "candidate" images. The bigger the pool of "candidates," the longer it takes to find a match—and the larger the pool of possible matches will likely be.

Performing matching, like everything else in facial recognition, requires significant computation resources. "Given how fast computers have become, it's not that much of an issue," said Aarabi. "If you narrow down a database to 10 million potential matches, which can be done in a reasonably short amount of time, so matching is not really a bottleneck anymore."

According to some National Institute of Standards and Technology benchmarks performed in 2010(PDF), "Using the most accurate face recognition algorithm, the chance of identifying the unknown subject (at rank 1) in a database of 1.6 million criminal records is about 92 percent." But the study found that for larger data sets, such as the FBI's 12 million image database, the accuracy of searches rapidly degrades. "For other population sizes, this accuracy rate decreases linearly with the logarithm of the population size. In all cases a secondary (human) adjudication process will be necessary to verify that the top-rank hit is indeed that hypothesized by the system," the authors of the study wrote.

Under ideal conditions, a facial recognition scan can at least come close to how such things play out in the movies. And even though facial recognition requires significant computing power to pull off, cloud computing and improved graphics processing are making it a lot easier to deploy—even to consumer devices. In testimony before the Senate Judiciary Committee last July, MorphoTrust's Martin told senators, "The technology is currently at a state where these face recognition algorithms can be deployed in anything from cell phones to large multiserver search engines capable of searching over 100 million faces in just a few seconds with operational accuracy."

## That driver's license photo is worse than you think

All that search speed, however, depends on the quality of the images in the database. Simply put, "if you don't have a good database, [you] won't get a match," Aarabi said. There's more to having a good facial database than having the suspect's picture in it.

Part of the problem investigators faced was that the facial database that did have images of at least one of the suspected bombers in it was built for a very specific purpose—preventing people from obtaining fraudulent driver's licenses.

Originally provided by Digimarc ID Systems started in 2006, the Massachusetts Registry of Motor Vehicles' facial recognition system is currently maintained (thanks to a series of corporate acquisitions) by MorphoTrust USA. The system, purchased with a $1.5 million grant from the Department of Homeland Security, holds images of the more than four million licensed drivers in the state of Massachusetts. It regularly catches as many as a thousand fraudulent license applicants every year.

"The DMV systems, they essentially have facial recognition in place because they want to prevent fraud with people trying to get licenses under different names," said Martin. "There are two cases that they typically use facial recognition in—the first is when you apply for a new license. They check against the database of images to see if they get a hit for someone under a different name. Then some human examiner goes through to see if there is a fraud case. The second case is to ensure, if you've had three or four licenses in the past, that your new one matches those past licenses."

In both of these scenarios, Martin said, "The capture of the photo is pretty controlled. You're looking at the camera with a flash and looking directly at the camera, so you can get really high accuracy."

Because the faces being matched are all in the same format, with the same lighting, and of essentially the samḋ resolution, the Registry's system is the facial recognition equivalent of shooting fish in a barrel. Even so, a bad match occasionally manages to squeak by. That's what happened to John Gass.

In 2011, Gass' license was revoked by the Registry of Motor Vehicles when another driver's image matched his enough to fool the system—and likely the inspector who checked the results. He ended up suing the state for loss of wages because of the 10-day ordeal he went through to prove that he was, in fact, a unique being. This sort of case is "incredibly rare," Martin said.

But when applied to the task of locating a terrorism suspect, the Registry's database is less than ideal. Despite their relatively perfect capture of each person's forward-looking face, all its photos of individuals are from the same angle.

There's also the issue of how that face changes. Dzhokhar Tsarnaev's drivers license photo was taken when he was 16; his facial structure may have changed during the last three years as he grew. And while many photos of Tsarnaev emerged once he was determined to be a suspect, the early images that law enforcement had to work with were less than ideal for matching up against a driver's license photo.

"If they had the driver's license image, it was a few years old, and they might have looked much different, and might not have been able to get a match from blurry surveillance image of the guy," said Martin. "It was a relatively hard case for face recognition. With some of the later images that came out, they weren't impossible to work with, and I think the technology could have come up with a match. But the ones the FBI posted on the website, I don't think there was a chance for matching them. It was too hard."

Inevitably, it came down to time. As more images were collected, a positive facial identification could have been made for Dzhokhar Tsarnaev—images were combined and a more detailed composite was assembled. But the desire to quickly apprehend the brothers led to the FBI publishing the surveillance images on April 18, hoping that the images would spur tips from the public. They ended up inspiring the Tsarnaevs' attempted flight. That ordeal contained many incidents authorities would likely want to forget: the killing of an MIT police officer, a car-jacking, and a shootout with police. According to law enforcement accounts, that last incident saw another policeman wounded and Tamerlan Tsarnaev shot; he was then run over by his brother in the stolen vehicle.

## Uncontrolled environments

Surveillance video of the Tsarnaev brothers captured by a retailer's surveillance camera near Copley Square.

There were a lot of pictures taken of the Tsarnaev brothers on April 15—some of them blurry, many of them not. But few of them were good candidates in the early hours of the investigation for getting a good match against a driver's license photo. Many of the best images came from digital surveillance systems set up at Lord & Taylor and other retailers near the bombings. Sadly, those cameras weren't in the best position to get a clean shot at the brothers' faces either. "These were uncontrolled environments," said 3VR's Karahashi. "In case of Boston bombing, you have so much raw footage, and they were processing video from cameras that weren't designed to be capturing faces." There were plenty of megapixel surveillance cameras in the mall, stores, and hotels around Copley Square—"but there [were] also a lot of analog and VGA resolution cameras," Karahashi said.

Some of those cameras were intended to capture faces, just not of people passing outside. Retailers, banks, and casino operators are among the businesses who have made the biggest investments in video surveillance, footage analysis, and facial recognition technology. Casinos in Las Vegas were among—largely to help them keep "undesirables" off their gaming floors—and they have invested heavily in video analysis systems that watch gaming tables for regulatory purposes or track car license plates as they go in and out of garages. Retailers and banks want to capture people's faces for similar reasons: "loss prevention" in retail, regulatory purposes, and security in banking. But retailers also want to be able to use surveillance footage to improve marketing and track customer behavior in their stores.

"In a store, you know people are going to come into [the] store through specific entrances, and [you] know that they'll be about a certain height, so if I have this camera angle, I'll have a pretty good rate capturing faces," said Karahashi.

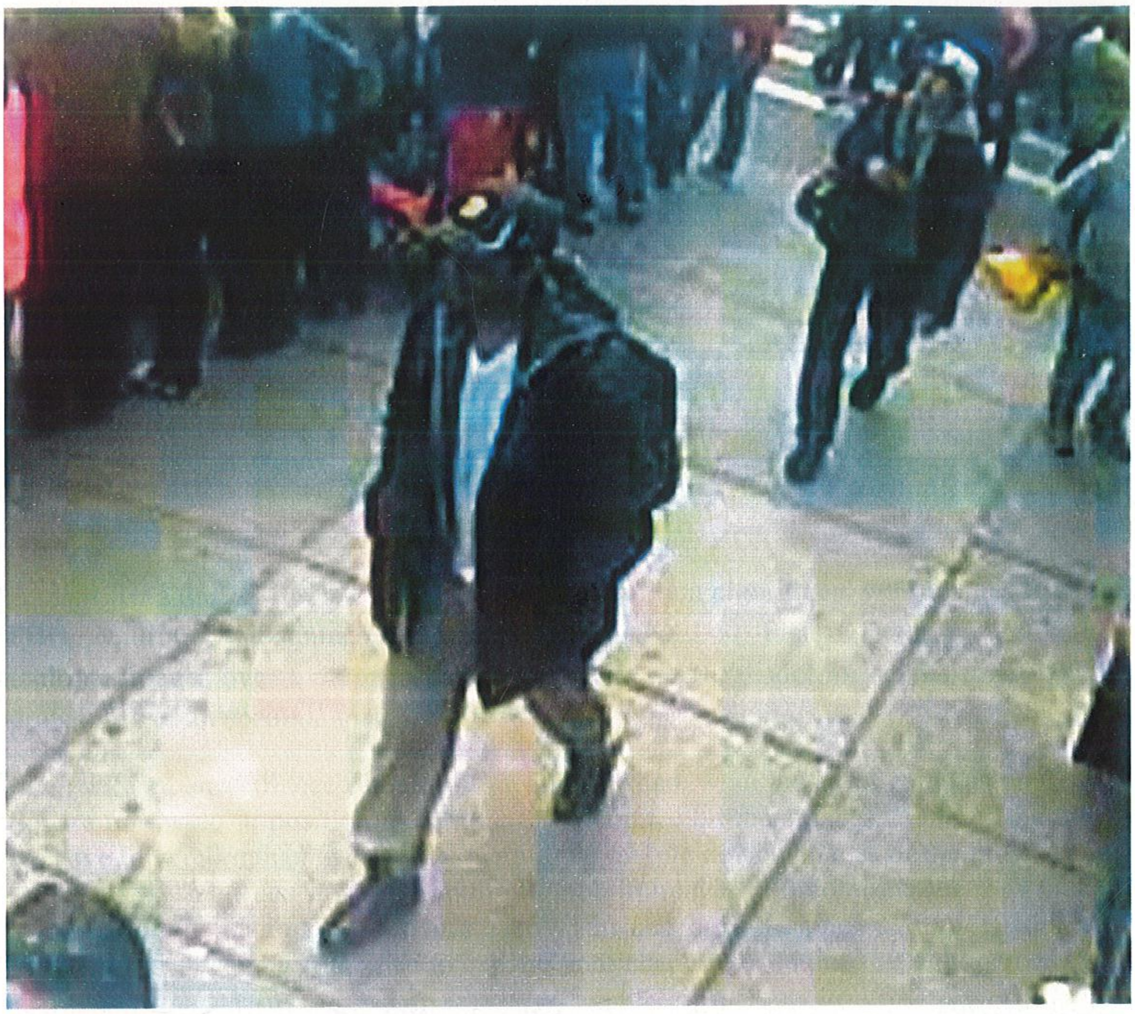
Video analysis systems can categorize and track individuals across multiple video feeds. But they can also pull in other sources of time-indexed data for context—such as transactions, alarms, and other events in a company's information systems.

Retailers can watch individuals walk the floor in a playback and see what they bought, if anything, and then adjust marketing to improve their "conversion rate." If someone calls a bank to complain about fraudulent ATM transactions, Karahashi said, a bank can pull up video footage from ATMs at the time of the transaction to spot the person making them. They can then use that person's image to search for other incidents across the entire network. A single complaint could uncover a broader ATM skimming operation.

But those scenarios all play out within a single system, and the digital cameras in Lord & Taylor and other stores couldn't capture the faces of passers-by unless they "volunteered their faces," Karahashi said.

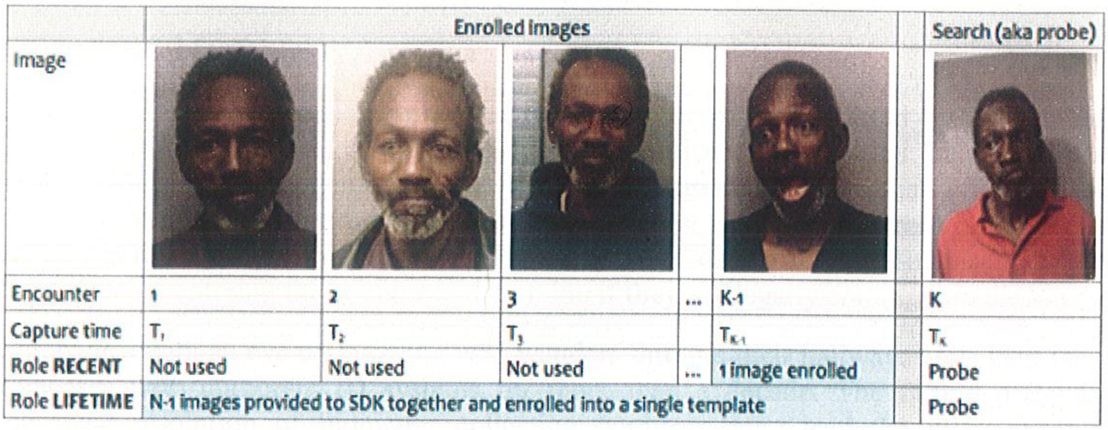
One of the early images of Dzhokhar Tsarnaev released by the FBI. The profile image would have been useless in a facial recognition search of the Massachusetts Registry of Motor Vehicles database.

Another early image released by the FBI. The low resolution of this image would have made a false negative—a total miss in the search—more likely, according to experts.



The angle of the footage from this retailer's surveillance camera, in combination with lighting, the sunglasses worn by Tamerlan Tsarnaev, and the ball caps worn by both of the brothers would have made a facial match difficult.

## Crowdsourcing the cameras, beefing up the database



| | Enrolled images | | | | | Search (aka probe) |
|---|---|---|---|---|---|---|
| Image | | | | | | |
| Encounter | 1 | 2 | 3 | ... | K-1 | K |
| Capture time | $T_1$ | $T_2$ | $T_3$ | | $T_{K-1}$ | $T_K$ |
| Role **RECENT** | Not used | Not used | Not used | ... | 1 image enrolled | Probe |
| Role **LIFETIME** | N-1 images provided to SDK together and enrolled into a single template | | | | | Probe |

A chart from the 2010 NIST study of facial recognition algorithms, with images from the FBI's Multiple Encounter, Deceased Subject (MEDS) facial database. Converting multiple images over time of an individual into a single model for search improved the probability of an accurate match.

Even without surveillance cameras at face-level, there were plenty of cameras on Copley Square that were in position to capture the Tsarnaev brothers' faces. "One of the things we have now more than ever before is multiple mobile device images of the same scene," said Aarabi. "You can now take multiple mobile images and combine them to make a high-resolution image of a person's face—you can have 10 photos from 10 different angles and they can be combined to expand your chances of finding the right person."

But if the goal is to have the ability to pull the name of someone on a surveillance camera feed out of the air at an instant, the problem may not be solved by more surveillance cameras. As NIST pointed out in its study of facial recognition, "multimode biometrics"—the combination of multiple images and characteristics of a person—can dramatically improve the value of biometric databases. Just having multiple photos of a person in the database from different angles and with different facial expressions can significantly improve the probability of a match.

Current systems "are not complex enough," said Kushan Ahmadian, an Alberta-based software developer who received his PhD in computer science studying biometrics and facial recognition. "If you use video and record their movement pattern at the time you take their picture, it significantly improves the quality of recognition."

Martin agrees that multimode can help. With high-resolution cameras, multiple biometrics can be collected by the same camera. He said iris recognition could be combined with facial recognition in some applications, since high-resolution cameras can pick up iris patterns in photos. According to Martin, researchers are even looking at using skin pores for identification. "If you have a high-enough resolution image, you can detect pore patterns that are unique to an individual that would distinguish him even from an identical twin," he said.

**License and (biometric) registration**

This sort of mult-mode biometric identification is already being used by the Defense Department and law enforcement agencies. The military widely used iris recognition along with photo recognition to record the identities of individuals in Iraq and Afghanistan. Police departments have begun to collect iris data on arrestees, and irises are part of the biometrics used by the DHS's US-VISIT database. That database is used to screen people entering the country to determine if they're illegally coming into the US.

Companies with an eye on knowing who wanders through their hallways have kept facial databases with corporate ID systems for more than a decade. The falling price and improved resolution of biometric collection hardware may lead the more security-conscious to increase the capabilities of their digital identity databases—especially as facial recognition systems become incorporated into login credentials. Financial institutions are starting to look at facial recognition systems to reduce transaction fraud. In April, the London-based software firm Facebanx introduced a technology that will let customers submit their own facial image to be added to their account information via webcam or mobile device to increase their accounts' security. Healthcare organizations are looking at scans for more reliable patient identification.

No one is standing in line at the DMV for multiple digital mug shots and iris scans yet. But with the technology within reach and demands for better surveillance voiced after the Boston bombing, it may soon become routine to get your pores and irises recorded by the DMV in addition to a front and side photo. It's a development with massive implications for security. Sadly, there's no guarantee you'll like your picture any better.

# TOOLS USED

**MATLAB** (**mat**rix **lab**oratory) is a numerical computing environment and fourth-generation programming language. Developed by MathWorks, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages,including C, C++, Java,Fortran.

# HISTORY

## Recent Improvements

In 2006, the performances of the latest face recognition algorithms were evaluated in the Face Recognition Grand Challenge (FRGC). High-resolution face images, 3-D face scans, and iris images were used in the tests. The results indicated that the new algorithms are 10 times more accurate than the face recognition algorithms of 2002 and 100 times more accurate than those of 1995. Some of the algorithms were able to outperform human participants in recognizing faces and could uniquely identify identical twins.

U.S. Government-sponsored evaluations and challenge problems have helped spur over two orders-of-magnitude improvement in face-recognition system performance. Since 1993, the error rate of automatic face-recognition systems has decreased by a factor of 272. The reduction applies to systems that match people with face images captured in studio or mugshot environments. In Moore's terms, the error rate decreased by one-half every two years.

Low-resolution images of faces can be enhanced using face hallucination. Further improvements in high resolution, megapixel cameras in the last few years have helped to resolve the issue of insufficient resolution.

## Early Improvement

Pioneers of Automated Facial Recognition include: Woody Bledsoe, Helen Chan Wolf, and Charles Bisson.

During 1964 and 1965, Bledsoe, along with Helen Chan and Charles Bisson, worked on using the computer to recognize human faces (Bledsoe 1966a, 1966b; Bledsoe and Chan 1965). He was proud of this work, but because the funding was provided by an unnamed intelligence agency that did not allow much publicity, little of the work was published. Given a large database of images (in effect, a book of mug shots) and a photograph, the problem was to select from the database a small set of records such that one of the image records matched the photograph. The success of the method could be measured in terms of the ratio of the answer list to the number of records in the database. Bledsoe (1966a) described the following difficulties:

This recognition problem is made difficult by the great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc. Some other attempts at facial recognition by machine have allowed for little or no variability in these quantities. Yet the method of correlation (or pattern matching) of unprocessed optical data, which is often used by some researchers, is certain to fail in cases where the variability is great. In particular, the correlation is very low between two pictures of the same person with two different head rotations.

This project was labelled man-machine because the human extracted the coordinates of a set of features from the photographs, which were then used by the computer for recognition. Using a graphics tablet (GRAFACON or RAND TABLET), the operator would extract the coordinates of features such as the centre of pupils, the inside corner of eyes, the outside corner of eyes, point of widows peak, and so on. From these coordinates, a list of 20 distances, such as width of mouth and width of eyes, pupil to pupil, were computed. These operators could process about 40 pictures an hour. When building the database, the name of the person in the photograph was associated with the list of computed distances and stored in the computer. In the recognition phase, the set of distances was compared with the corresponding distance for each photograph, yielding a distance between the photograph and the database record. The closest records are returned.

This brief description is an oversimplification that fails in general because it is unlikely that any two pictures would match in head rotation, lean, tilt, and scale (distance from the camera). Thus, each set of distances is normalized to represent the face in a frontal orientation. To accomplish this normalization, the program first tries to determine the tilt, the lean, and the rotation. Then, using these angles, the computer undoes the effect of these transformations on the computed distances. To compute these angles, the computer must know the three-dimensional geometry of the head. Because the actual heads were unavailable, Bledsoe (1964) used a standard head derived from measurements on seven heads.

After Bledsoe left PRI in 1966, this work was continued at the Stanford Research Institute, primarily by Peter Hart. In experiments performed on a database of over 2000 photographs, the computer consistently outperformed humans when presented with the same recognition tasks (Bledsoe 1968). Peter Hart (1996) enthusiastically recalled the project with the exclamation, "It really worked!"

By about 1997, the system developed by Christoph von der Malsburg and graduate students of the University of Bochum in Germany and the University of Southern California in the United States outperformed most systems with those of Massachusetts Institute of Technology and the University of Maryland rated next. The Bochum system was developed through funding by the United States Army Research Laboratory. The software was sold as ZN-Face and used by customers such as Deutsche Bank and operators of airports and other busy locations. The software was "robust enough to make identifications from less-than-perfect face views. It can also often see through such impediments to identification as moustaches, beards, changed hair styles and glasses—even sunglasses".

In about January 2007, image searches were "based on the text surrounding a photo," for example, if text nearby mentions the image content. Polar Rose technology can guess from a photograph, in about 1.5 seconds, what any individual may look like in three dimensions, and thought they "will ask users to input the names of people they recognize in photos online" to help build a database.

## Iris Recognition

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the irides of an individual's eyes, whose complex random patterns are unique and can be seen from some distance.

Not to be confused with another, less prevalent, ocular-based technology, retina scanning, iris recognition uses camera technology with subtle infrared illumination to acquire images of the detail-rich, intricate structures of the iris. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual. Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per (single-core) CPU, and with infinitesimally small False Match rates.

Many millions of persons in several countries around the world have been enrolled in iris recognition systems, for convenience purposes such as passport-free automated border-crossings, and some national ID systems based on this technology are being deployed. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to False Matches, is the stability of the iris as an internal, protected, yet externally visible organ of the eye.

In 1987 two Ophthalmology Professors, Leonard Flom, M.D.(NYU) and Aran Safir,M.D.(U.Conn), were issued a first of its kind, broad patent # 4,641,349 entitled "Iris Recognition Technology." Subsequently, John Daugman,PhD (Harvard Computer Science faculty) was then salaried by both ophthalmologists to write the algorithm for their concept based upon an extensive series of high resolution iris photos supplied to him by Dr.Flom from his volunteer private patients. Several years later, Daugman received a method patent for the algorithm and a crudely constructed prototype proved the concept. The three individuals then founded "Iridian Technologies,Inc." and assigned the Flom/Safir patent to that entity that was then capitalized by GE Capital, a branch of "GE"(General Electric) and other investors.

"Iridian" then licensed several corporations to the exclusive Daugman algorithm under the protection of the Flom/Safir broad umbrella patent listed above; thus, preventing other algorithms from competing. Upon expiration of the Flom/Safir patent in 2008 other algorithms were patented and several were found to be superior to Daugman's and are now being funded by U.S. Government agencies.

# CHAPTER-1

# FACE DETECTION

# DESCRIPTION

Face detection can be regarded as a specific case of object-class detection. In object-class detection, the task is to find the locations and sizes of all objects in an image that belong to a given class. Examples include upper torsos, pedestrians, and cars.

Face detection can be regarded as a more general case of face localization. In face localization, the task is to find the locations and sizes of a known number of faces (usually one). In face detection, one does not have this additional information.

Many algorithms implement the face-detection task as a binary pattern-classification task. That is, the content of a given part of an image is transformed into features, after which a classifier trained on example faces decides whether that particular region of the image is a face, or not.

Often, a window-sliding technique is employed. That is, the classifier is used to classify the (usually square or rectangular) portions of an image, at all locations and scales, as either faces or non-faces (background pattern).

Images with a plain or a static background are easy to process. Remove the background and only the faces will be left, assuming the image only contains a frontal face. Using skin colour to find face segments is a vulnerable technique. The database may not contain all the skin colours possible. Lighting can also affect the results. Non-animate objects with the same colour as skin can be picked up since the technique uses colour segmentation. The advantages are the lack of restriction to orientation or size of faces and a good algorithm can handle complex backgrounds.

Faces are usually moving in real-time videos. Calculating the moving area will get the face segment. However, other objects in the video can also be moving and would affect the results. A specific type of motion on faces is blinking. Detecting a blinking pattern in an image sequence can detect the presence of a face. Eyes usually blink together and symmetrically positioned, which eliminates similar motions in the video. Each image is subtracted from the previous image. The difference image will show boundaries of moved pixels. If the eyes happen to be blinking, there will be a small boundary within the face.

A face model can contain the appearance, shape, and motion of faces. There are several shapes of faces. Some common ones are oval, rectangle, round, square, heart, and triangle. Motions include, but not limited to, blinking, raised eyebrows, flared nostrils, wrinkled forehead, and opened mouth. The face models will not be able to represent any person making any expression, but the technique does result in an acceptable degree of accuracy. The models are passed over the image to find faces, however this technique works better with face tracking. Once the face is detected, the model is laid over the face and the system is able to track face movements.

A method for human face detection from colour videos or images is to combine various methods of detecting colour, shape, and texture. First, use a skin colour model to single out objects of that colour. Next, use face models to eliminate false detections from the colour models and to extract facial features such as eyes, nose, and mouth.

## SKIN COLOUR SEGMENTATION

The goal of skin color segmentation is to reject non-skin color regions from the input image. It is based on the fact that the color of the human face across all races agrees closely in its chrominance value and varies mainly in its luminance value.

We used the YCbCr color space for segmentation. Each input tile is converted from the RGB color space to the YCbCr color space. The transform used takes an RGB input value with each component in the range [0-255] and transforms it into Y, Cb, and Cr, in the ranges [0.0, 255.0], [-128.0, 127.0], and [-128.0, 127.0], respectively. The Y-component is level-shifted down by 128, so that it also falls into the [-128.0, 127.0] range. The input tile in this level-shifted symmetric YCbCr color space is used as the input for the next stage of DWT. The matrix equation for this conversion is shown in the

$$[Y \quad Cb \quad Cr] = [R \quad G \quad B] \begin{bmatrix} 0.299 & -0.168935 & 0.499813 \\ 0.587 & -0.331665 & -0.418531 \\ 0.114 & 0.50059 & -0.081282 \end{bmatrix}$$

following figure.

The threshold values were embedded into the color segmentation routine.

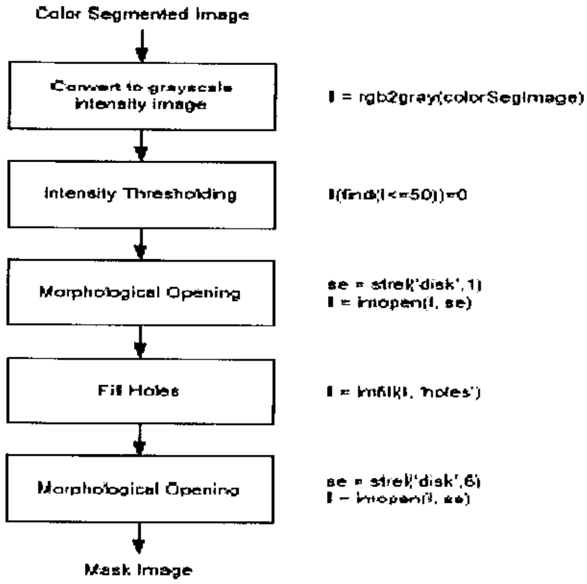
During the execution of the detector, segmentation is performed as follows:

1. The input image is converted to YCbCr color space
2. All pixels that fall outside the Cb and Cr thresholds are rejected (marked black).
3. Then we create a binary mask of the segmented image.

The result is shown in image 2(appendix).

## MORPHOLOGICAL PROCESSING

Image 2(Appendix) shows that skin color segmentation did a good job of rejecting non-skin colors from the input image. However, the resulting image has quite a bit of noise and clutter. A series of morphological operations are performed to clean up the image, as shown in below Figure. The goal is to end up with a mask image that can be applied to the input image to yield skin color regions without noise and clutter.



```
I = rgb2gray(colorSegImage)
I(find(I<=50))=0
se = strel('disk',1)
I = imopen(I, se)
I = imfill(I, 'holes')
se = strel('disk',6)
I = imopen(I, se)
```

A description of each step is as follows:

1. Since morphological operations work on intensity images, the color segmented image is converted into a gray image.
2. Intensity thresholding is performed to break up dark regions into many smaller regions so that they can be cleaned up by morphological opening. The threshold is set low enough so that it doesn't chip away parts of a face but only create holes in it.
3. Morphological opening is performed to remove very small objects from the image while preserving the shape and size of larger objects in the image. The definition of a morphological *opening* of an image is an erosion followed by a dilation, using the same structuring element for both operations. A disk shaped structuring element of radius 1 is used.

4. Hole filling is done to keep the faces as single connected regions in anticipation of a second much larger morphological opening. Otherwise, the mask image will contain many cavities and holes in the faces.
5. Morphological opening is performed to remove small to medium objects that are safely below the size of a face. A disk shaped structuring element of radius 6 is used.

# CONNECTED REGION ANALYSIS

The image output by morphological processing still contains quite a few non-face regions. Most of these are hands, arms, regions of dress that match skin color and some portions of background. In connected region analysis, image statistics from the training set are used to classify each connected region in the image.

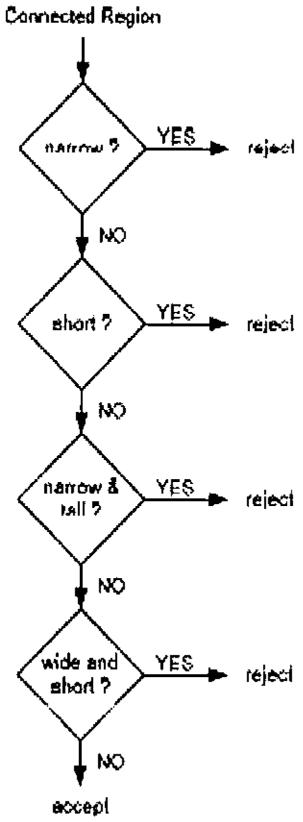
## Rejection based on Geometry

We used four classes of regions that have a very high probability of being non-faces based on their bounding box:

| | |
|---|---|
| • narrow | Regions that have a small width |
| • short | Regions that have a small height |
| • narrow and tall | Regions that have a small width but large height |
| • wide and short | Regions that have a large width but small height |

We did not use the wide and tall class because that interferes with large regions that contain multiple faces.

Based on the training set image statistics, thresholds were calculated for each class. The constraints were then applied in the following order:



## Rejection based on Euler number

The Euler number of an image is defined as the number of objects in the image minus the total number of holes in those objects. Euler number analysis is based on the fact that regions of the eyes, nose and lips are distinctively darker from other face regions and show up as holes after proper thresholding in the intensity level.
An adaptive scheme is used to generate the threshold for each connected region. First, the mean and the standard deviation of the region's intensity level is calculated. If there is a large spread (i.e. ratio of mean to standard deviation is high), the threshold is set to a fraction of the mean. This prevents darker faces from breaking apart into multiple connected regions after thresholding. Otherwise, the threshold is set higher (some multiple of the standard deviation) to make sure bright faces are accounted for.

The thresholded region is used to compute its Euler number e. If e >= 0 (i.e. less than two holes) we reject the region. This is because the face has at least two holes corresponding to the eyes.

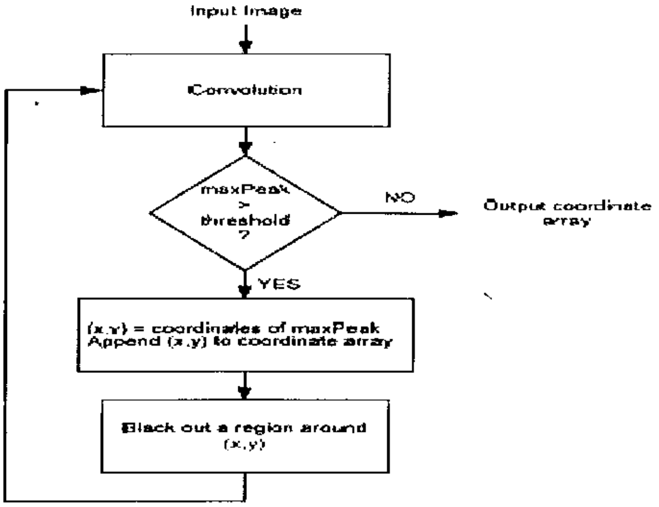
# TEMPLATE MATCHING

The basic idea of template matching is to convolve the image with another image (template) that is representative of faces. Finding an appropriate template is a challenge since ideally the template (or group of templates) should match any given face irrespective of the size and exact features.

The template was originally generated by cropping off all the faces in the training set using the ground truth data and averaging over them. The intensity image obtained after color segmentation contained faces with a neck region and so we need to modify out template to include the neck region. This is done by taking the intensity image after color segmentation, separating out the connected regions, then manually selecting the faces and averaging over them.

Once we convolved the intensity image obtained from connected region analysis with our template. The results will be reasonable for regions with a single face, as convolution gave a high peak for these regions. However, for regions containing a bunch of faces clustered together, a simple convolution isn't that effective. One obvious problem is how to detect the convolution peaks. Another one is that faces hidden behind other faces didn't register a high enough value to show up as peaks. It is also noticed that template matching was highly dependent on the shape of the template and not so much on the features, so that using a single face as a template actually gave poorer results. A drawback of this was that regions similar in shape to a face also resulted in convolution peaks.

Instead of doing a single convolution and detecting the peaks, we need a convolution, that looked at the coordinates of the maximum peak, blacked out a rectangular region (similar in size to the template) around those coordinates and repeated the same process again till the maximum peak value was below a specified threshold.


Input Image
Convolution
maxPeak > threshold ?
NO
Output coordinate array
YES
(x,y) = coordinates of maxPeak
Append (x,y) to coordinate array
Black out a region around (x,y)

# RESULTS AND CONCLUSIONS

We have made efforts towards developing a face detector with a reasonably good accuracy and running time. However, many aspects of the design are tuned for the constrained scene conditions of the image provided, hurting its robustness.

The image outputs of various procedures performed have been extremely useful results for the development of the project. The images show accurately the result after the procedure has been performed. Though our project has not been completed, we look forward to finish it as soon as possible.
We feel that detecting connected faces was the hardest part of the project.

# Advantages and Disadvantages of Facial Recognition

For people who understand how facial recognition works, this comes as no surprise. Despite advances in the technology, systems are only as good as the data they're given to work with. Real life isn't like anything you may have seen on *NCIS* or *Hawaii Five-0*. Simply put, facial recognition isn't an instantaneous, magical process. Video from a gas station surveillance camera or a police CCTV camera on some lamppost cannot suddenly be turned into a high-resolution image of a suspect's face that can then be thrown against a drivers' license photo database to spit out an instant match.

Not yet. Facial recognition technology has gotten a lot better in the past decade, and the addition of other biometric technologies to facial recognition is making it increasingly accurate. Facial recognition and other biometric and image processing technologies, such as gait recognition, helped law enforcement find the suspects in the rush of people with the help of retailers' own computerized surveillance systems.

The fact is that it's much more likely for a bank or department store to know who you are when you walk past a camera than for law enforcement to make an ID based on video footage. That's because you give retailers a lot more information to work with—and the systems they use are arguably better suited to keeping track of you than most police surveillance systems.

Further the database management of huge populous will have an impact over the searching for the required match though even the facial recognition is very fast.

Uncontrolled environmental challenges like breach of privacy, very low lighting conditions would not be effective and thus limit our workforce of thorough analysis of the images required for the personnel and further using image-registration approach adding more cost could help us to overcome this low light conditions.

Advantages and future advances in biometrics:

- Less intrusiveness makes it easier to implement & adding a more secure environment.
- Faster technique to sort out the particulars of the suspect.
- Very simple approach that uses three basic methods of classification.
- More successful biometric systems integrate Iris, face, voice detection to make it more sophisticated and adding more versatile types of biometric recognition techniques such as voice and fingerprint helps us to boost our security

# APPLICATIONS

## • Government Use

- Law Enforcement. Minimizing victim trauma by narrowing mugshot searches, verifying identify for court records, and comparing school surveillance camera images to known child molesters.
- Security/Counterterrorism. Access control, comparing surveillance images to known terrorists.
- Immigration. Rapid progression through Customs.
- Legislature. Verify identity of Congressmen prior to vote.
- Correctional institutions/prisons. Inmate tracking, employee access.

## • Commercial Use

- Day Care. Verify identity of individuals picking up the children.
- Missing Children/Runaways. Search surveillance images and the internet for missing children and runaways.
- Gaming Industry. Find card counters and thieves.
- Residential Security. Alert homeowners of approaching personnel.
- Internet, E-commerce. Verify identity for Internet purchases.
- Healthcare. Minimize fraud by verifying identity.
- Benefit payments. Minimize fraud by verifying identity.
- Voter verification. Minimize fraud by verifying identity.
- Banking. Minimize fraud by verifying identity.

# CHAPTER-2
# IRIS RECOGNITION

# DESCRIPTION

Popularity of the iris biometric grew considerably over the past three years. The problems of processing, encoding Iris texture, and designing iris-based recognition systems have attracted the attention of a large number of research teams. On the other side, the iris biometric has been gaining public acceptance. Modern cameras used for iris acquisition are less intrusive compared to earlier iris scanning devices. Iridology is the science of analyzing the delicate structures of the iris of the eye. The iris reveals body constitution, inherent weaknesses, and levels of health and transitions that take place in a person's body according to the way one lives. There is an old saying that the eyes are the window of the soul. They can also be a window to one's health. Like fingerprints or faces, no two irises (the colored part of the eye) are exactly alike. The iris structure is so unique it is now being used for security identification at ATM machines and airports. And for centuries, it has also been used to analyze people's health – past, present and future. The study of the iris for medical purposes is called iridology. The iris contains detailed fibers and pigmentation that reflects our physical and psychological makeup. When an organ or body system is in poor health, the nerve running from that body part will start to recede. When it does, it draws with it various degrees of the layers of fibers which make up the color of the iris of the eyes, leaving darkened marks called lesions. Iris is one the important Biometric Identification technique and also Iris is one of unique identifier of Human then it is stable throughout a life of the person's. In this work, a new method to recognition of the eye has been proposed.

# IRIS ANATOMY

The iris is responsible for regulating the amount of light that enters the pupil and is absorbed by the retina. The amount of light that enters the pupil is regulated through the constriction or dilation of the pupil. Since the pupil has no mechanism to regulate its shape on its own the iris, through the contraction of muscles, provides the required movement. The process of mydriasis is the dilation of the pupil by the dilator pupillae muscle which is triggered by activity in the parasympathetic nerve in low lighting conditions. On the contrary, in the presence of intense light the pupil will contract. The contraction is caused by a process called miosis where the constrictor pupillae muscle, triggered by the parasympathetic nerve, reduces the amount of light which enters the pupil.

The iris is the only internal human organ which is visible from the outside of the body allowing it to be easily imaged. The ease of imaging makes iris an ideal biometric. The iris is formed prenatally, independent of genetic genotype. The process is considered to be random, unique, chaotic and only dependent on initial conditions in the embryonic mesoderm. Due to the chaotic and random nature of the iris and the ability to easily acquire a contact-less image, the iris is considered to be a strong biometric.

# IRIS STRUCTURE

Due to the vibrant color and texture of the iris it is typically the most visible and distinguishable part of the human eye. The average diameter of the iris is approximately 12mm with an average thickness around 5mm. The iris is thickest at the collarette and continues to thin out radially as you move away from the pupil. The truncated cone shape of the iris is due to the anterior surface of the lens pressing against the posterior iris.

Irides are composed of firbrovascular tissue known as stroma. A stroma connects the sphincter pupillae, which contracts the pupil, and the dilator pupillae, responsible for dilating the pupil. The dilator pupillae, a dilator muscle, and the sphincter pupillae, a sphincter muscle, are a group of muscles which are found in irides of all vertebrates. The back surface of the iris is covered by the iris pigment epithelium. The surface is covered by an epithelial layer which is two cells thick and results in the color of the iris. The front (outside) surface of the iris does not consist of a epithelium layer. The root of the iris is the outer edge of the iris and attaches the sclera to the anterior ciliary body of the iris. The sclera is the opaque (typically white) fibrous, protective layer of the eye which comprises majority of the iris surface. The ciliary body, together with the iris, known as the anterior uvea, is the circumferential tissue inside the eye (Figure 2.1)1.The ciliary body is mostly responsible for providing most of the nutrients to the lens and cornea as well as conducting waste management for the same areas. The region of the iris in front of the root is responsible for drainage of aqueous humour, crucial to the maintenance of the eye. Aqueous humour is a thick watery substance responsible for in°ating the globe of the eye and providing nutrition for the avascular ocular tissues.

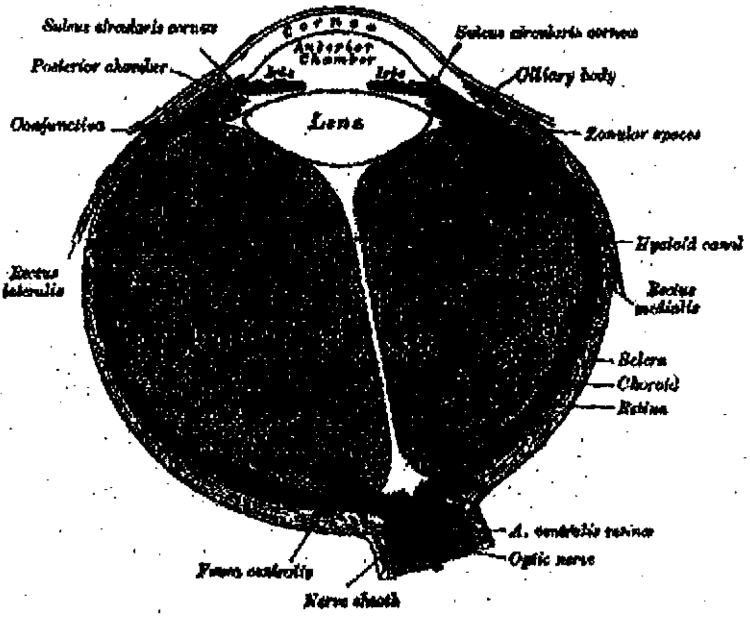


Figure 2.1: Dissection of a human eye showing the structures of the eye

The iris is divided into two major regions (Figure 2.2): pupillary zone and ciliary zone. The pupillary zone is the inner region of the iris which ends at the boundary of the pupil. The ciliary zone extends from its origin to the ciliary body. The collarette is the region where the sphincter muscle and dilator muscle overlap. This is considered the point at which the pupillary portion and ciliary portion interchange. Iris color as well as structural features often vary between the two zones. Fruch's crypts are openings which appear on either side of the collarette and allows stroma and other deep iris tissue to be submerged in aqueous humor during dilation and contraction of the pupil. Though these features are common on both portions of the outer iris they are much more common in the ciliary zone of the iris.

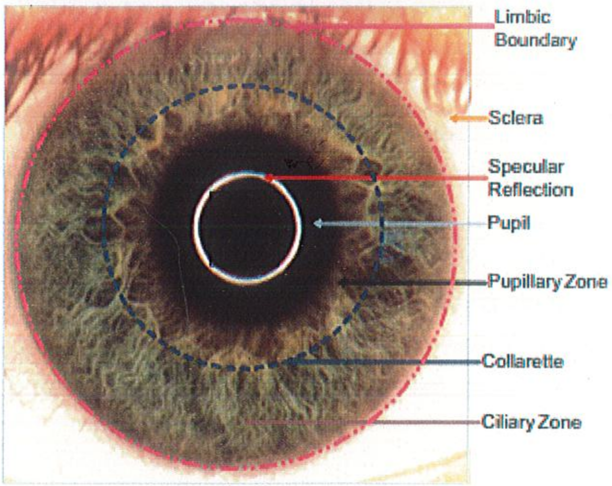


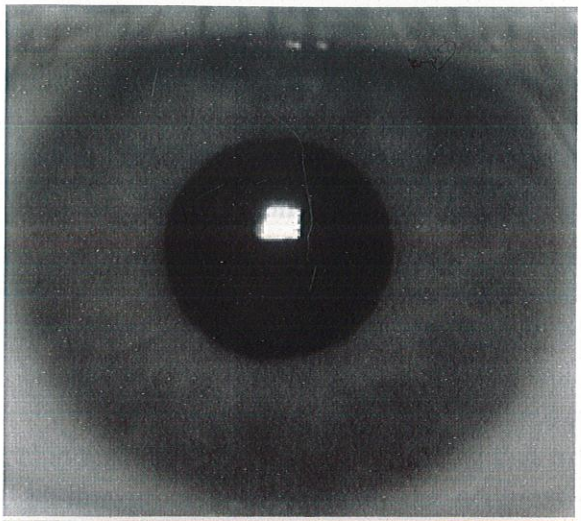
Figure 2.2: Major regions of the visible iris

The iris is comprised of six layers starting from the anterior(front) to the posterior(back). The layers are as follows: anterior border layer, stroma of iris, iris sphincter muscle, iris dilator muscle, anterior pigment myoepithelium and the posterior pigment epithelium. The anterior portion of the iris is the focus of most recognition systems due to accessability for imaging.

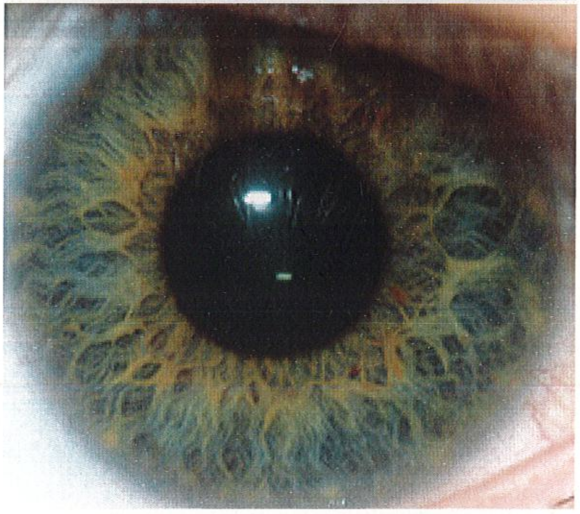
# Visible Wavelength (VW) vs. Near Infrared (NIR) Imaging

Most iris recognition systems acquire images of the iris in the visible wavelength (400-700 nm) or near infrared range (700 - 900 nm) of the electromagnetic spectrum. Each wavelength distinguishes different features of the iris with NIR and VW obtaining Information from the iris by its texture and pigmentation, respectively. The majority of iris recognition systems operate within the longer NIR spectrum which can penetrate dark-coloured irides, the dominant phenotype of the human population, revealing texture not easily observed in the VW spectrum.

## Comparison between Visible Wavelength (VW) vs. Near Infrared (NIR) Imaging



Pigmentation of the Iris is much less visible due to the negligible effects of Melanin at longer wavelengths in the NIR spectrum



Visible light reveals rich pigmentation details of an Iris by exciting Melanin, the main colouring component in the iris.

# IMAGE ACQUISITION

One of the major challenges of automated iris recognition is to capture a high-quality image of the iris while remaining noninvasive to the human operator. Given that the iris is a relatively small (typically about 1 cm in diameter), dark object and that human operators are very sensitive about their eyes, this matter requires careful engineering. Several points are of particular concern. First, it is desirable to acquire images of the iris with sufficient resolution and sharpness to support recognition. Second, it is important to have good contrast in the interior iris pattern without resorting to a level of illumination that annoys the operator, i.e., adequate intensity of source constrained by operator comfort with brightness. Third, these images must be well framed (i.e., centered) without unduly constraining the operator (i.e., preferably without requiring the operator to employ an eye piece, chin rest, or other contact positioning that would be invasive). Further, as an integral part of this process, artifacts in the acquired images (e.g., due to specular reflections, optical aberrations, etc.) should be eliminated as much as possible. Schematic diagrams of two image-acquisition rigs that have been developed in response to these challenges.

# ADVANTAGES

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons:

It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor.

The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face.

The iris has a fine texture that—like fingerprints—is determined randomly during embryonic gestation. Like the fingerprint, it is very hard (if not impossible) to prove that the iris is unique. However, there are so many factors that go into the formation of these textures (the iris and fingerprint) that the chance of false matches for either is extremely low. Even genetically identical individuals have completely independent iris textures.

An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person being identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against fingerprint scanners, where a finger has to touch a surface, or retinal scanning, where the eye must be brought very close to an eyepiece (like looking into a microscope).

The commercially deployed iris-recognition algorithm, John Daugman's IrisCode, has an unprecedented false match rate (better than 10−11 if a Hamming distance threshold of 0.26 is used, meaning that up to 26% of the bits in two IrisCodes are allowed to disagree due to imaging noise, reflections, etc., while still declaring them to be a match).

## Major short comings of Iris Recognition systems:

Many commercial iris scanners can be easily fooled by a high quality image of an iris or face in place of the real thing.

The scanners are often tough to adjust and can become bothersome for multiple people of different heights to use in succession.

The accuracy of scanners can be affected by changes in lighting

Iris scanners are significantly more expensive than some other forms of biometrics, password or prox card security systems

Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition.

Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera. However, several academic institutions and biometric vendors are developing products that claim to be able to identify subjects at distances of up to 10 meters ("standoff iris" or "iris at a distance" as well as "iris on the move" for persons walking at speeds up to 1 meter/sec).

As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates.

As with other identification infrastructure (national residents databases, ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will.

Researchers have tricked iris scanners using images generated from digital codes of stored irises. Criminals could exploit this flaw to steal the identities of others.

Alcohol consumption causes recognition degradation as the pupil dilates/constricts causing deformation in the iris pattern.

While there are some medical and surgical procedures that can affect the colour and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years.

# ALGORITHM USED

## Segmentation

The first stage of iris recognition is to isolate the actual iris region in a digital eye image. The iris region, can be approximated by two circles, one for the iris/sclera boundary and another, interior to the first, for the iris/pupil boundary. The eyelids and eyelashes normally occlude the upper and lower parts of the iris region. Also, specular reflections can occur within the iris region corrupting the iris pattern. A technique is required to isolate and exclude these artefacts as well as locating the circular iris region.

Various Techniques:

- Hough Transform
- Daugman's Integro-differential operator
- Active contour models
- Eyelash and Noise detection

## Normalisation

Once the iris region is successfully segmented from an eye image, the next stage is to transform the iris region so that it has fixed dimensions in order to allow comparisons. The dimensional inconsistencies between eye images are mainly due to the stretching of the iris caused by pupil dilation from varying levels of illumination. Other sources of inconsistency include, varying imaging distance, rotation of the camera, head tilt, and rotation of the eye within the eye socket. The normalisation process will produce iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at the same spatial location.

Another point of note is that the pupil region is not always concentric within the iris region, and is usually slightly nasal. This must be taken into account if trying to normalise the 'doughnut' shaped iris region to have constant radius.

Various Techniques:

- Daugman's rubber sheet model
- Image registration
- Virtual circles

## Feature Encoding and Matching

In order to provide accurate recognition of individuals, the most discriminating information present in an iris pattern must be extracted. Only the significant features of the iris must be encoded so that comparisons between templates can be made. Most iris recognition systems make use of a band pass decomposition of the iris image to create a biometric template.

The template that is generated in the feature encoding process will also need a corresponding matching metric, which gives a measure of similarity between two iris templates. This metric should give one range of values when comparing templates generated from the same eye, known as intra-class comparisons, and another range of values when comparing templates created from different irises, known as inter-class comparisons. These two cases should give distinct and separate values, so that a decision can be made with high confidence as to whether two templates are from the same iris, or from two different irises.

Various Techniques of Encoding:

- Wavelet encoding
- Gabor filters
- Log-gabor filters

Various Techniques of Matching:

- Hamming distance
- Weighted Euclidean Distance
- Normalised correlation

# RESULTS AND CONCLUSION

We have made efforts towards developing a iris detector with a reasonably good accuracy and running time. However, many aspects of the design are tuned for the constrained scene conditions of the image provided, hurting its robustness.

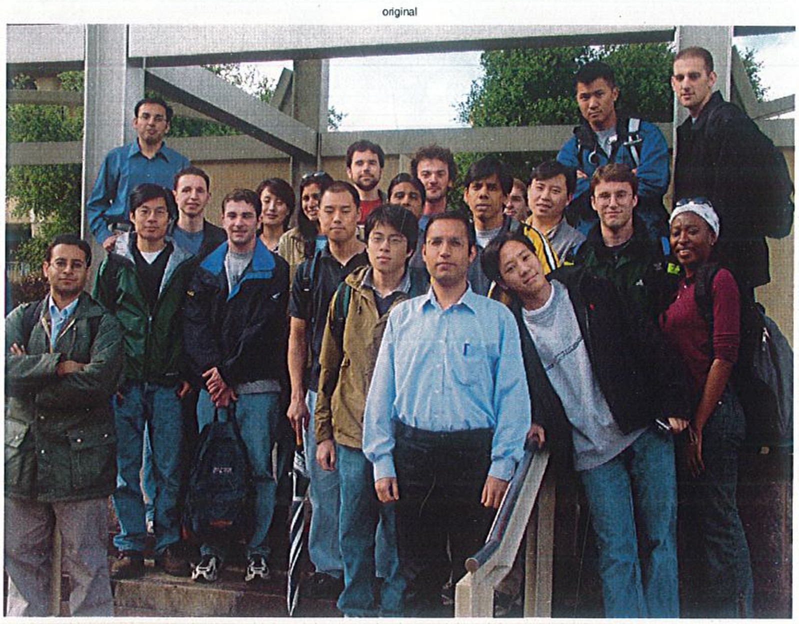
The image outputs of various procedures performed have been extremely useful results for the development of the project. The images show accurately the result after the procedure has been performed. Though our project has not been completed, we look forward to work on it as soon as possible.

Iris Extraction and recognition system has been developed steadily with the help of MATLAB and some mathematical calculations, however limitations such as blur and dynamically taken images make it impossible to achieve perfect naturalness to combat this, we need to take images in ultraviolet environment. After getting image from the user the system will detect iris part of human eye, system applied various inbuilt MATLAB functions and mathematical calculations to encircle outer part of pupil that is inner part of iris and will mark the outer part of iris.

# APPENDICES

# Chapter-1

## LIST OF OUTPUT IMAGES



Input Image
Image 1

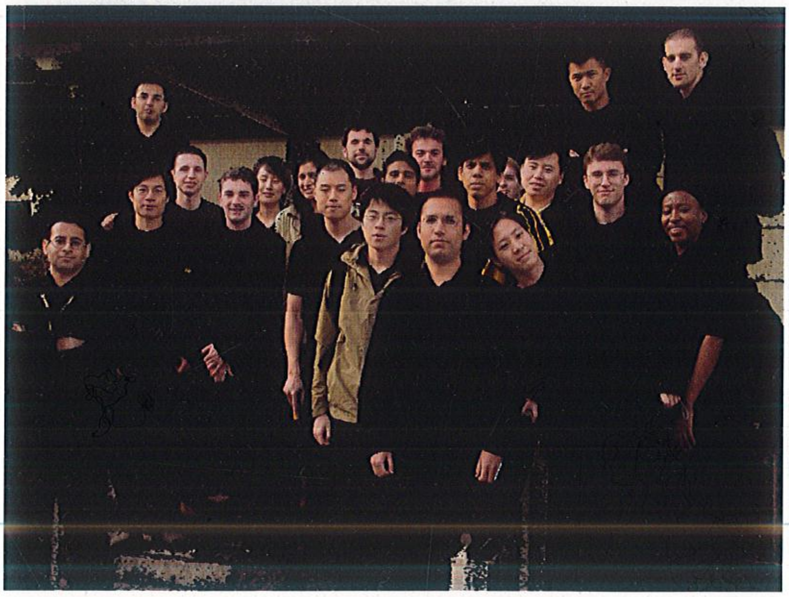
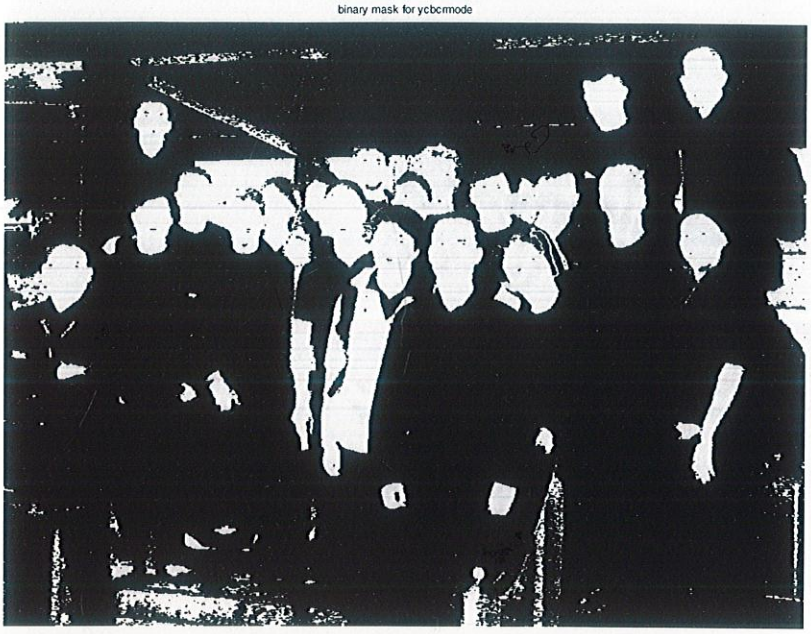


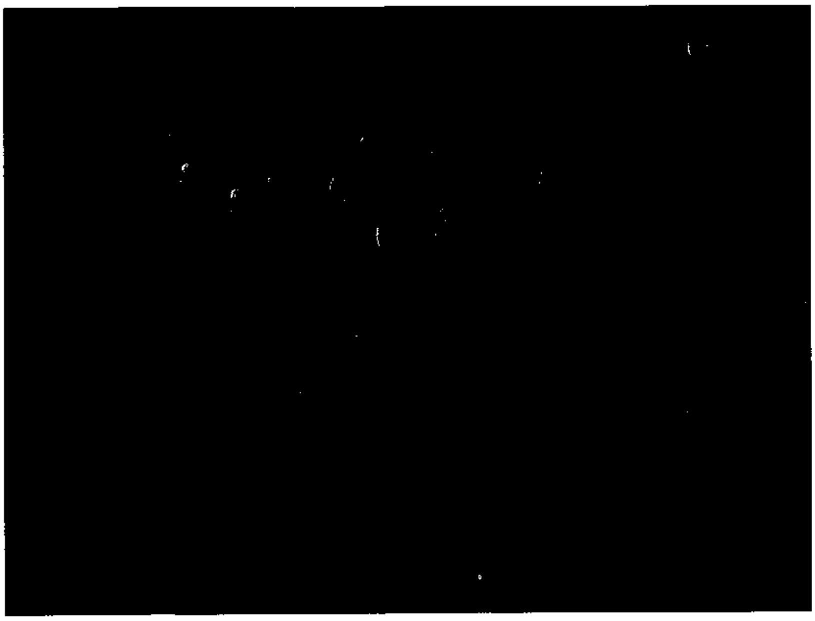
Image after Colour Segmentation

Image 2



Binary Mask of Colour Segmented Image
Image 3

Image after Morphological Processing
Image 4



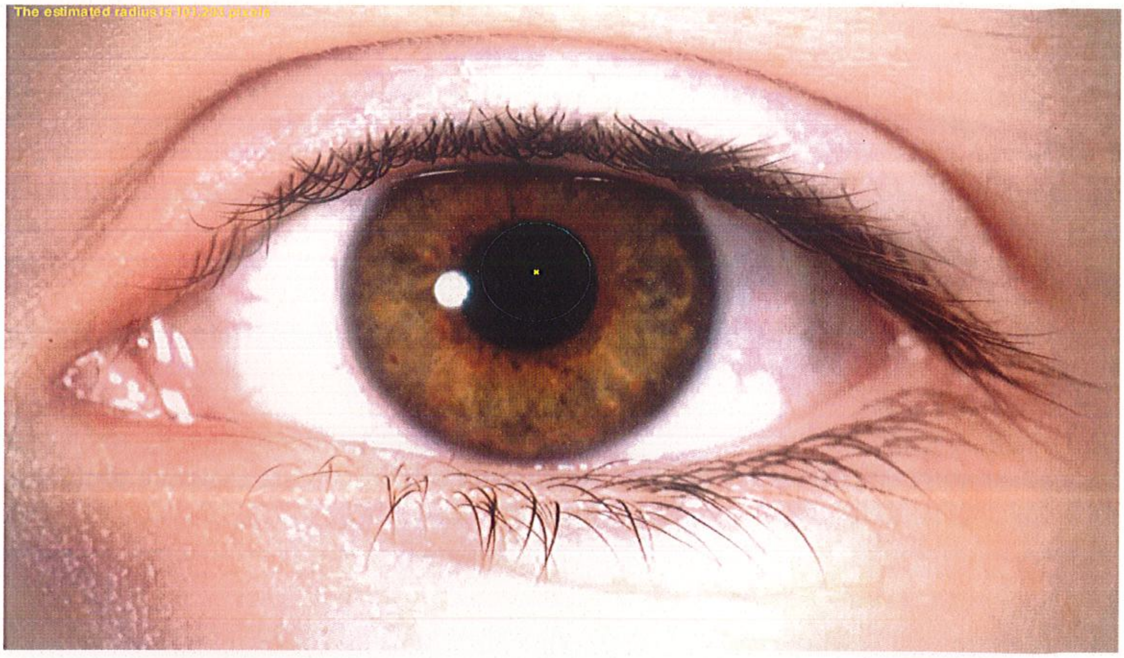
Bounded regions for Connected Region Analysis
Image 5

## MATLAB CODE

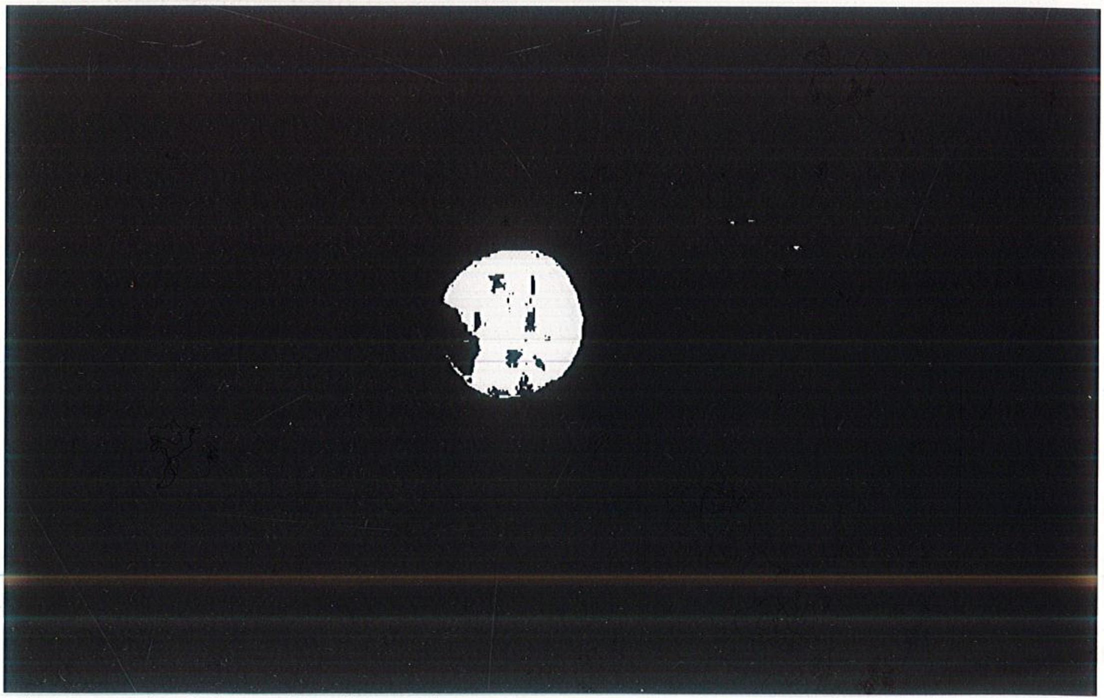
```
clc;
img=imread('image1.jpg');
imshow(img),title('original');
img;
m = size(img,1);
n = size(img,2);
p = size(img,3);
img2=img;

%image conversion from rgb to ycbcr
img1=rgb2ycbcr(img);
ycbcr_skin = zeros(m,n);
r=img(:,:,1);
g=img(:,:,2);
b=img(:,:,3);
y=img1(:,:,1);
cb=img1(:,:,2);
cr=img1(:,:,3);
cr1=133;
cr2=173;
cb1=77;
cb2=127;

for i = 1:m
for j = 1:n
 if(cr(i,j)>cr1 && cr(i,j)<cr2 && cb(i,j)>cb1 &&cb(i,j)<cb2)
   ycbcr_skin(i,j)=1;
 else
    img2(i,j,1)=0;
    img2(i,j,2)=0;
    img2(i,j,3)=0;
end
end
end
figure;imshow(img2);

%creating a binary mask
final_ycbcr = zeros(m,n);
for i = 1:m
for j = 1:n
if(ycbcr_skin(i,j)==1)
   final_ycbcr(i,j)=img(i,j);
end
```

```
end
end
figure;imshow(final_ycbcr),title('binary mask for ycbcrmode');

%morphological processing
i=rgb2gray(img2);
i(find(i<=50))=0;
se=strel('disk',1);
i=imopen(i,se);
i=imfill(i,'holes');
se=strel('disk',6);
i=imopen(i,se);
figure;imshow(i);

%connected region analysis
%rejection based on geometry
BW = i;
[b,~,N] = bwboundaries(BW);
figure; imshow(BW); hold on;
for k=1:length(b)
   boundary = b{k};
   if(k > N)
      plot(boundary(:,2),...
         boundary(:,1),'g','LineWidth',2);
   else
      plot(boundary(:,2),...
         boundary(:,1),'r','LineWidth',2);
   end
end
L = bwlabel(BW);
s = regionprops(L, 'BoundingBox');
crops=cell(62,1);
for x=1:length(s)
   subimage = imcrop(L, s(x,1).BoundingBox);
   crops(x,1)={subimage;};
end
for x=1:62
dim=size(crops{x,1});
width{x,1}=dim(2);
length{x,1}=dim(1);
end
for x=1:62
  if (100>length{x,1} || length{x,1}>200 || 100>width{x,1} || width{x,1}>200)
   for y=1:1:62
      for z=1:1:62
      i=b{y,1}(z,1);
      j=b{y,1}(z,2);
      BW(i{z,1},j{z,1},1)=0;
      BW(i{z,1},j{z,1},2)=0;
      BW(i{z,1},j{z,1},3)=0;
      i=0;
      j=0;
      end
   end
  end
end
figure; imshow(BW);
```

## LIST OF OUTPUT IMAGES



Input image identifying the iris radius and centroid



Binary mask of the region detected

## MATLAB CODE

```
i=imread('e.jpg');
imshow(i)

ir=i(:,:,1);
ig=i(:,:,2);
ib=i(:,:,3);
[a b c]=size(i);
for m=1:a
   for n=1:b

if(ir(m,n)>=3&&ir(m,n)<=28&&ig(m,n)>=3&&ig(m,n)<=28&&ib(m,n)>=6&&ib(m,n)<
=30);
        j(m,n)=1;
      else
         j(m,n)=0;
      end
   end
end
imview(j);

[l,num]=bwlabel(j);
if(num>0)
   stats=regionprops(l,'Basic');
   max_area=max([stats.Area]);
big=find([stats.Area]==max_area);
loc=stats(big).Centroid;
else
   loc=[0 0];
end
cx=0;
cy=0;
cx=loc(1,1);
cy=loc(1,2);
disp(cx);
disp(cy);
dim = size(j);
col = round(dim(2)/2)-90;
row = find(j(:,col), 1);
connectivity = 8;
num_points   = 180;
contour = bwtraceboundary(j, [row, col], 'N', connectivity, num_points);
imshow(i);
hold on;
```

```
plot(contour(:,2),contour(:,1),'g','LineWidth',1);


x = contour(:,2);
y = contour(:,1);

% solve for parameters a, b, and c in the least-squares sense by
% using the backslash operator
abc = [x y ones(length(x),1)] \ -(x.^2+y.^2);
a = abc(1); b = abc(2); c = abc(3);

% calculate the location of the center and the radius
xc = -a/2;
yc = -b/2;
radius  =  sqrt((xc^2+yc^2)-c)

% display the calculated center
plot(xc,yc,'yx','LineWidth',2);

% plot the entire circle
theta = 0:0.01:2*pi;

% use parametric representation of the circle to obtain coordinates
% of points on the circle
Xfit = radius*cos(theta) + xc;
Yfit = radius*sin(theta) + yc;

plot(Xfit, Yfit);

message = sprintf('The estimated radius is %2.3f pixels', radius);
text(15,15,message,'Color','y','FontWeight','bold');
BWoutline = bwperim(i);
Segout = i;
Segout(BWoutline) = 255;
figure, imshow(Segout), title('outlined original image');
```

# References:

[1] Ruiping Wang, Member, IEEE, Shiguang Shan, Member, IEEE, Xilin Chen, Senior Member, IEEE, Qionghai Dai, Senior Member, IEEE, and Wen Gao, Fellow, IEEE, "Manifold-Manifold Distance and Its Application to Face Recognition with Image Sets", IEEE paper.

[2] Rick Kjeldsen and John Kender, "Finding Skin in Colour Images", IEEE Transactions, 1996.

[3] C. Garcia and G. Tziritas, "Face detection using quantized skin colour region merging and packet analysis," IEEE Transactions on Multimedia Vol.1, No. 3, pp. 264--277, September 1999.

[4] The Face Detection Homepage, http://home.t-online.de/home/Robert.Frischholz/index.html.

[5] Standford university submissions, http://www.stanford.edu/class/ee368/Project_03/Project/reports/ee368group10.pdf.

[6] Francesa Gasparini, Raimondo Schettini, 'Skin segmentation using multiple thresholding', http://www.ivl.disco.unimib.it/papers2003/EI06-EI109%20Skin-paper.pdf.

[7] Mansi Jhamb, Vinod Kumar Khera, "IRIS based human recognition system", IEEE Transactions, 2010.

[8] Mathew K. Monaco, "Color space analysis for IRIS recognition", Thesis, http://csee.wvu.edu/IIAS/docs/thesis/monaco-thesis.pdf

[9] John G. Daugman, "High Confidence Visual recognition of persons by a test of statistical independence", IEEE Transactions on pattern analysis and machine intelligence, vol.15, No.11, November 1993.