INSTITUTE OF ROAD AND TRANSPORT TECHNOLOGY

ERODE-638316

**FACE RECOGNITION**

**(pattern matching & bio-metrics)**

**CATEGORY- IMAGE PROCESSING**



**Submitted by,**

**G.MEGALA**

**R.KIRUTHIGA**

**Third year-CSE**

**Email:** [**megala.deva95**](mailto:joystephy45@gmai.com)**@gmail.com**

**Kirutirk95@gmail.com**

**Phone no:9659694536**

**9095471228**

**ABSTRACT:**

**Government agencies are investing a considerable amount of resources into improving security systems as result of recent terrorist events that dangerously exposed flaws and weaknesses in today’s safety mechanisms. Badge or password-based authentication procedures are too easy to hack. Biometrics represents a valid alternative but they suffer of drawbacks as well. Iris scanning, for example, is very reliable but too intrusive; fingerprints are socially accepted, but not applicable to non-consentient people. On the other hand, face recognition represents a good compromise between what’s socially acceptable and what’s reliable, even when operating under controlled conditions. In last decade, many algorithms based on linear/nonlinear methods, neural networks, wavelets, etc. have been proposed. Nevertheless, Face Recognition Vendor Test 2002 shown that most of these approaches encountered problems in outdoor conditions. This lowered their reliability compared to state of the art biometrics.**

**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 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:**

|  |
| --- |
|  |

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.

Identix®, a company based in Minnesota, is one of many developers of facial recognition technology. Its software, FaceIt®, can pick someone's face out of a crowd, extract the face from the rest of the scene and compare it to a database of stored images. In order for this software to work, it has to know how to differentiate between a basic face and the rest of the background. Facial recognition software is based on the ability to recognize a face and then measure the various features of the face.

Every face has numerous, distinguishable **landmarks**, the different peaks and valleys that make up facial features. FaceIt defines these landmarks as **nodal points**. Each human face has approximately 80 nodal points. Some of these measured by the software are:

* Distance between the eyes
* Width of the nose
* Depth of the eye sockets
* The shape of the cheekbones
* The length of the jaw line

These nodal points are measured creating a numerical code, called a **face print**, representing the face in the database.

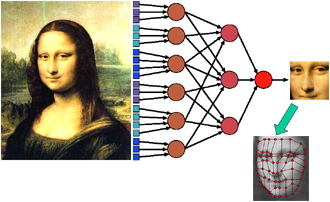
|  |
| --- |
| **Photo** [**.**](http://computer.howstuffworks.com/framed.htm?parent=facial-recognition.htm&url=http://identix.com) **FaceIt software compares the face print with other images in the database.** |

In the past, facial recognition software has relied on a 2D image to compare or identify another 2D image from the database. To be effective and accurate, the image captured needed to be of a face that was looking almost directly at the camera, with little variance of light or facial expression from the image in the database. This created quite a problem.

In most instances the images were not taken in a controlled environment. Even the smallest changes in light or orientation could reduce the effectiveness of the system, so they couldn't be matched to any face in the database, leading to a high rate of failure. In the next section, we will look at ways to correct the problem.

**TECHNOLOGY**

Our technology is based on neural computing and combines the advantages of elastic and neural networks.  
Neural computing provides technical information processing methods that are similar to the way information is processed in biological systems, such as the human brain. They share some key strengths, like robustness fault-resistance and the ability to learn from examples. Elastic networks can compare facial landmarks even if images are not identical, as is practically always the case in real-world situations. Neural networks can learn to recognize similarities through pattern recognition.



# 3D FACIAL RECOGNITION

|  |
| --- |
|  |

A newly-emerging trend in facial recognition software uses a 3D model, which claims to provide more accuracy. Capturing a real-time 3D image of a person's facial surface, 3D facial recognition uses distinctive features of the face -- where rigid tissue and bone is most apparent, such as the curves of the eye socket, nose and chin -- to identify the subject. These areas are all unique and don't change over time.

Using depth and an axis of measurement that is not affected by lighting, 3D facial recognition can even be used in darkness and has the ability to recognize a subject at different view angles with the potential to recognize up to 90 degrees (a face in profile).

Using the 3D software, the system goes through a series of steps to verify the identity of an individual.

**Detection**  
Acquiring an image can be accomplished by digitally scanning an existing photograph (2D) or by using a video image to acquire a live picture of a subject (3D).

**Alignment**

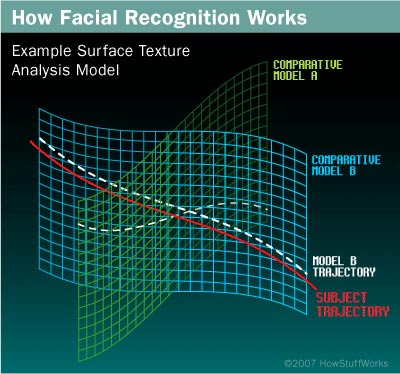
Once it detects a face, the system determines the head's position, size and pose. As stated earlier, the subject has the potential to be recognized up to 90 degrees, while with 2D, the head must be turned at least 35 degrees toward the camera.

**Measurement**  
The system then measures the curves of the face on a sub-millimeter (or microwave) scale and creates a template.

|  |
| --- |
|  |

**Representation**  
The system translates the template into a unique code. This coding gives each template a set of numbers to represent the features on a subject's face.

**Matching**  
If the image is 3D and the database contains 3D images, then matching will take place without any changes being made to the image. However, there is a challenge currently facing databases that are still in 2D images. 3D provides a live, moving variable subject being compared to a flat, stable image. New technology is addressing this challenge. When a 3D image is taken, different points are identified. For example, the outside of the eye, the inside of the eye and the tip of the nose will be pulled out and measured. Once those measurements are in place, an algorithm will be applied to the image to convert it to a 2D image. After conversion, the software will then compare the image with the 2D images in the database to find a potential match.



The surface texture analysis (STA) algorithm operates on the top percentage of results as determined by the local feature analysis. STA creates a skin print and performs either a 1:1 or 1:N match depending on wether you're looking for verification or identification.

**Verification or Identification**  
In verification, an image is matched to only one image in the database (1:1). For example, an image taken of a subject may be matched to an image in the Department of Motor Vehicles database to verify the subject is who he says he is. If identification is the goal, then the image is compared to all images in the database resulting in a score for each potential match (1:N). In this instance, you may take an image and compare it to a database of mug shots to identify who the subject is.

Next, we'll look at how skin biometrics can help verify matches.

# SURFACETEXTURE ANALYSIS

The image may not always be verified or identified in facial recognition alone. Identix® has created a new product to help with precision. The development of FaceIt®Argus uses skin biometrics, the uniqueness of skin texture, to yield even more accurate results.

The process, called Surface Texture Analysis, works much the same way facial recognition does. A picture is taken of a patch of skin, called a skin print. That patch is then broken up into smaller blocks. Using algorithms to turn the patch into a mathematical, measurable space, the system will then distinguish any lines, pores and the actual skin texture. It can identify differences between identical twins, which is not yet possible using facial recognition software alone. According to Indenter, by combining facial recognition with surface texture analysis, accurate identification can increase by 20 to 25 percent.

FaceIt currently uses three different templates to confirm or identify the subject: vector, local feature analysis and surface texture analysis.

* The vector template is very small and is used for rapid searching over the entire database primarily for one-to-many searching.
* The local feature analysis (LFA) template performs a secondary search of ordered matches following the vector template.
* The surface texture analysis (STA) is the largest of the three. It performs a final pass after the LFA template search, relying on the skin features in the image, which contains the most detailed information.

By combining all three templates, FaceIt® has an advantage over other systems. It is relatively insensitive to changes in expression, including blinking, frowning or smiling and has the ability to compensate for mustache or beard growth and the appearance of [eyeglasses](http://science.howstuffworks.com/lens.htm). The system is also uniform with respect to race and gender.

|  |
| --- |
|  |

However, it is not a perfect system. There are some factors that could get in the way of recognition, including:

* Significant glare on eyeglasses or wearing sunglasses
* Long hair obscuring the central part of the face
* Poor lighting that would cause the face to be over- or under-exposed
* Lack of resolution (image was taken too far away)

Identix isn't the only company with facial recognition systems available. While most work the same way FaceIt does, there are some variations. For example, a company called Animetrix, Inc. has a product called FACEngine ID® SetLight that can correct lighting conditions that cannot normally be used, reducing the risk of false matches. Sensible Vision, Inc. has a product that can secure a computer using facial recognition. The computer will only power on and stay accessible as long as the correct user is in front of the screen. Once the user moves out of the line of sight, the computer is automatically secured from other users.

# CURRENT & FUTURE USES OF FACIAL RECOGNITION SYSTEMS

# ****The ideal solution**** All of this makes face recognition ideal for high traffic areas open to the general public, such as: - Airports and railway stations - Casinos - Cash points - Stadiums - Public transportation - Financial institutions - Government offices - Businesses of all kinds

In the past, the primary users of facial recognition software have been law enforcement agencies, who used the system to capture random faces in crowds. Some government agencies have also been using the systems for security and to eliminate voter fraud. The U.S. government has recently begun a program called US-VISIT (United States Visitor and Immigrant Status Indicator Technology), aimed at foreign travelers gaining entry to the United States. When a foreign traveler receives his visa, he will submit fingerprints and have his photograph taken. The fingerprints and photograph are checked against a database of known criminals and suspected terrorists. When the traveler arrives in the United States at the port of entry, those same fingerprints and photographs will be used to verify that the person who received the visa is the same person attempting to gain entry.

**Hard to fool**  
  
Face recognition is also very difficult to fool. It works by comparing facial landmarks - specific proportions and angles of defined facial features - which cannot easily be concealed by beards, eyeglasses or makeup.

However, there are now many more situations where the software is becoming popular.

* As the systems become less expensive, making their use more widespread.
* They are now compatible with cameras and computers that are already in use by banks and airports. Registered Traveler program will provide speedy security screening for passengers who volunteer information. At the airport there will be specific lines for the Registered Traveler to go through that will move more quickly, verifying the traveler by their facial features.
* Other potential applications include ATM and check-cashing security. After a customer consents, the ATM or check-cashing kiosk captures a digital image of him. The FaceIt software then generates a face print of the photograph to protect customers against identity theft and fraudulent transactions.
* By using the facial recognition software, there's no need for a picture ID, bankcard or personal identification number (PIN) to verify a customer's identity. This way business can prevent fraud from occurring.

**DRAWBACKS OF THIS TECHNOLOGY**

While all the examples above work with the permission of the individual, not all systems are used with your knowledge.

These systems were taking pictures of all visitors without their knowledge or their permission. Opponents of the systems note that while they do provide security in some instances, it is not enough to override a sense of liberty and freedom.

Many feel that privacy infringement is too great with the use of these systems, but their concerns don't end there.

They also point out the risk involved with [identity theft](http://people.howstuffworks.com/identity-theft.htm). Even facial recognition corporations admit that the more use the technology gets, the higher the likelihood of identity theft or fraud.

**CONCLUSION**

As with many developing technologies, the incredible potential of facial recognition comes with some drawbacks, but manufacturers are striving to enhance the usability and accuracy of the systems. Face recognition promises latest security invents in the upcoming trends based on bio-metrics and pattern matching techniques and algorithms.

**REFERENCES:**

## *"Using your body as a key; legal aspects of biometrics".*

## *Biometrics Consortuim.*

## Y. Adini, Y. Moses, and S. Ullman, “Face recognition: the problem of compensating for changes in illumination direction,” IEEE Trans. Pattern Anal. Machine Intell., vol. 19, pp. 721–732, July 1997.