# FACE RECOGNITION USING THE THEORY OF BIOMETRICS IMAGE PROCESSING

**MS. B Jayanthi*    K. Santhosh Kumar****
*\*Assistant Professor, Head department of Computer Science, RVS college of Arts and Science.*
*\*\*Assistant Professor, Providence College for Women, Coonoor.*

*Abstract*

*While humans have had the innate ability to recognize and distinguish different faces for millions of years, computers are just now catching up. In this paper, we'll learn how computers are turning your face into computer code so it can be compared to thousands, if not millions, of other faces. We'll also look at how face recognition software is being used in elections, criminal investigations and to secure your personal computer.*

*Face recognition software falls into a larger group of technologies known as biometrics. Biometrics uses biological information to verify identity. The basic idea behind biometrics is that our bodies contain unique properties that can be used to distinguish us from others. Face recognition methods may vary, but they generally involve a series of steps that serve to capture, analyze and compare your face to a database of stored images.*

*A Software company called Visionics developed face recognition software called Face it. The heart of this facial recognition system is the Local Feature Analysis (LFA) algorithm. This is the mathematical technique the system uses to encode faces. The system maps the face and creates a face print, a unique numerical code for that face. Once the system has stored a face print, it can compare it to the thousands or millions of face prints stored in a database. Potential applications even include ATM and check-cashing security, Security Law Enforcement & Security Surveillance. This biometrics technology could also be used to secure your computer files, by mounting a webcam to your computer and to get into your computer. By implementing this technology and the normal password security you are getting double security to your valuable data.*

*Key Words: Finger-scan, face recognition, Iris-scan, Retina-scan, and Hand-scan.*

## Introduction

People have an amazing ability to recognize and remember thousands of faces. While humans have had the innate ability to recognize and distinguish different faces for millions of years, computers are just now catching up. In this paper, you'll learn how computers are turning your face into computer code so it can be compared to thousands, if not millions, of other faces. We'll also look at how face recognition software is being used in elections, criminal investigations and to secure your personal computer. Biometrics is considered a natural means of identification since the ability to distinguish among individual appearances is possessed by humans.

Face-scan technology is based on the standard biometrics sequence of image acquisition, image acquisition, and image processing distinctive characteristic location, templates creations, and matching. An optimal image is captured through a high resolution camera, with moderate lighting and users directly facing a camera. The enrollment images define the facial characteristics to be used in all future verifications, thus a high quality enrollment is essential. Challenges that acquisition and lighting. Distance from the camera reduces facial size and thus image resolution.

**What is biometrics?**  A biometric is a unique, measurable characteristic of a human being that can be used to automatically recognize an individual or verify an individual's identity. Biometrics can measure both physiological and behavioral characteristics. Physiological biometrics (based on measurements and data derived from direct measurement of a part of the human body) include:

## The Face

Your face is an important part of who you are and how people identify you. Imagine how hard it would be to recognize an individual if all faces looked the same. Except in the case of identical twins, the face is arguably a person's most unique physical characteristic. While humans have had the innate ability to recognize and distinguish different faces for millions of years, computers are just now catching up. Visionics, a company based in New Jersey, is one of many developers of facial recognition technology. The twist to its particular software, Face It, is that it can pick someone's face out of a crowd, extract that face from the rest of the scene and compare it to a database full of stored images. In order for this software to work, it has to know what a basic face looks like. Face recognition software can be used to find criminals in a crowd, turning a mass of people into a big line up face recognition software is based on the ability to first recognize a face, which is a technological

feat in itself, and then measure the various features of each face. If you look in the mirror, you can see that your face has certain distinguishable landmarks. These are the peaks and valleys that make up the different facial features. Visionics defines these landmarks as nodal points. There are about 80 nodal points on a human face. Here are a few of the nodal points that are measured by the software: *Distance between eyes, Width of nose, Depth of eye sockets, Cheek bones, Jaw Line, Chin.* These nodal points are measured to create a numerical code, a string of numbers that represents the face in a database. This code is called a face print. Only 15 to 23 nodal points are needed for the Face It software to complete the recognition process. In the next section, we'll look at how the system goes about detecting, capturing and storing faces.

**The Software**
Face recognition software falls into a larger group of technologies known as biometrics. Biometrics uses biological information to verify identity. The basic idea behind biometrics is that our bodies contain unique properties that can be used to distinguish us from others. Besides face recognition, biometric authentication methods also include Fingerprint scan, Retina scan and Voice identification. Face recognition methods may vary, but they generally involve a series of steps that serve to capture, analyze and compare your face to a database of stored images. Here is the basic process that is used by the Face It system to capture and compare images**.** To identify someone, face recognition software compares newly captured images to databases of stored images.

**Detection**
When the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for faces. If there is a face in the view, it is detected within a fraction of a second. A multi-scale algorithm is used to search for faces in low resolution. (An algorithm is a program that provides a set of instructions to accomplish a specific task). The system switches to a high-resolution search only after a head-like shape is detected.

**Alignment**

Once a face is detected, the system determines the head's position, size and pose. A face needs to be turned at least 35 degrees toward the camera for the system to register it.

**Normalization**
The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose. Normalization is performed regardless of the head's location and distance from the camera. Light does not impact the normalization process.

**Representation**
The system translates the facial data into a unique code. This coding process allows for easier comparison of the newly acquired facial data to stored facial data.

**Matching**
The newly acquired facial data is compared to the stored data and (ideally) linked to at least one stored facial representation. The heart of the Face It facial recognition system is the Local Feature Analysis (LFA) algorithm. This is the mathematical technique the system uses to encode faces. The system maps the face and creates a face print, a unique numerical code for that face. Once the system has stored a face print, it can compare it to the thousands or millions of face prints stored in a database. Each face print is stored as an 84-byte file. The system can match multiple face prints at a rate of 60 million per minute from memory or 15 million per minute from hard disk. As comparisons are made, the system assigns a value to the comparison using a scale of one to 10. If a score is above a predetermined threshold, a match is declared. The operator then views the two photos that have been declared a match to be certain that the computer is accurate. Facial recognition, like other forms of biometrics, is considered a technology that will have many uses in the near future. In the next section, we will look how it is being used right now.

**Why we choose face recognition over other biometric?**
There are number reasons to choose face recognition. This includes the following:  It requires no physical interaction on behalf of the user.  It is accurate and allows for high enrolment and verification rates. It does not require an expert to interpret the comparison result.  It can use your existing hardware infrastructure, existing cameras and image capture Devices will work with no problems. It is the only biometric that allow you to perform passive identification in a one to.

## Implementation of Face Recognition Technology

The implementation of face recognition technology includes the following three stages:

- Data acquisition.
- Input processing.
- Face image classification and decision making.

## Applications

The primary users of face recognition software like Face It have been law enforcement agencies, which use the system to capture random faces in crowds. These faces are compared to a database of criminal mug shots. In addition to law enforcement and security surveillance, facial recognition software has several other uses, including: Eliminating voter fraud, Check-cashing identity verification, Computer security. One of the most innovative uses of facial recognition is being employed by the Mexican government, which is using the technology to weed out duplicate voter registrations. Potential applications even include ATM and check-cashing security. The software is able to quickly verify a customer's face. After the user consents, the ATM or check-cashing kiosk captures a digital photo of the customer. The face recognition software then generates a face print of the photograph to protect customers against identity theft and fraudulent transactions. By using face recognition software, there's no need for a picture ID, bank card or personal identification number (PIN) to verify customer's identity. This biometric technology could also be used to secure your computer files. By mounting a Webcam to your computer and installing the facial recognition software, your face can become the password you use to get into your computer.

## Advantages and Disadvantages

*Advantages*: There are many benefits to face recognition systems such as its convenience and Social acceptability. Face recognition is easy to use and in many cases it can be performed without a Person even knowing. Face recognition is also one of the most inexpensive biometric in the market and its price should continue to go down.

*Disadvantages*: Face recognition systems can't tell the difference between identical twins.

## Conclusion

With the following advantages and also some of the drawbacks, we conclude our paper on Face Recognition using Biometrics. Potential applications are as follows*: Eliminating voter fraud, Security law enforcement and Security surveillance, ATM and Check-cashing identity verification, Computer security.* While face recognition can be used to protect your private information, it can just as easily be used to invade your privacy by taking you picture when you are entirely unaware of the camera. As with many developing technologies, the incredible potential of face recognition comes with drawbacks. But if we add both the facial recognition and the normal password security we can have an added Double Security which is more reliable than one shield security.

## References

1. Morrison RL, Bellack AS, Mueser KT: Deficits in facial-affect recognition and schizophrenia. Schizophr Bull 1988; 14:67–83 2. Mandal MK, Pandey R, Prasad AB: Facial expressions of emotions and schizophrenia: review. Schizophr Bull 1998; 24:399– 412
2. Ekman P, Friesen WV: Manual of the Facial Action Coding System (FACS). Palo Alto, Calif, Consulting Psychologists Press, 1978
3. Lembke A, Ketter TA: Impaired recognition of facial emotion in mania. Am J Psychiatry 2002; 159:302–304
4. Gur RE, Turetsky BI, Cowell PE, Finkelman C, Maany V, Grossman RI, Arnold SE, Bilker WB, Gur RC: Temporolimbic volume reductions in schizophrenia. Arch Gen Psychiatry 2000; 57: 769–775
5. First MB, Spitzer RL, Gibbon M, Williams JB: Structured Clinical Interview for DSM-IV Axis I Disorders—Non-Patient Edition (SCID-I/NP), version 2.0. New York, New York State Psychiatric Institute, Biometrics Research, 1996