Aditi Uniyal, 2021, 9:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Face Recognition Using AI + BIOTECH

Aditi Uniyal, Dharmendra Bisht, Shivank Verma
School of Computer Science,
Galgotias University Gr. Noida, India
Uniyal.Ad@Gmail.Com, Dharmendrabisht2042001@Gmail.Com, Shivankverma1012@Gmail.Com

Abstract- How to accurately and effectively identify people has always been an interesting topic, both in research and in industry. With the rapid development of artificial intelligence in recent years, facial recognition gains more and more attention. Compared with the traditional card recognition, fingerprint recognition and iris recognition, face recognition has many advantages, including but limit to non-contact, high concurrency, and user friendly. It has high potential to be used in government, public facilities, security, e-commerce, retailing, education and many other fields. Accurate face recognition is critical for many security applications. Current automatic facerecognition systems are defeated by natural changes in lighting, pose and masks, which often affect face images more profoundly than changes in identity. The only system that can reliably cope with such variability is a human observer who is familiar with the faces concerned.We have discussed model human familiarity by using image averaging to derive stable face representations from naturally varying photographs. This process involves three stages: Pre-processing, Feature Extraction and Classification. The geometric features of facial images like eyes, nose, mouth etc. are located and face recognition is performed. This simple procedure can increase the accuracy of an industry standard face-recognition algorithm from 54% to 94%, bringing the robust performance of a familiar human to an automated system. We focus on importance of most successful solution available so far ,all together with its methods and uses also in areas not related to face recognition.

Keywords:- Face recognition, biometric identification, methods, applications.

I. INTRODUCTION

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearences.

Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN‟s and passwords: birthdays, phone numbers and social security numbers. Recent cases of identity theft have highten the need for methods to prove that someone is truly who he/she claims to be. Face recognition technology may solve this problem since a face is undeniably connected to its owner expect in the case of identical twins. Its non transferable.

The system can then compare scans to records stored in a central or local database or even on a smart card. Digital image processing is a rapidly evolving field with growing applications in science and engineering. Image processing holds the probability of developing the ultimate machine that could perform the visual function of all living beings.

II. 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.

1. Physiological Biometrics:
Physiological Biometrics (based on measurements and data derived from direct measurement of a part of the human body) include:

- Finger-scan
- Facial Recognition
- Iris-scan
- Retina-scan
- Hand-scan

2. Behavioral Biometrics:
This biometrics is based on measurements and data derived from an action.

- Voice-scan
- Signature-scan
- Keystroke-scan

III. 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 camaras 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. Many environments (e.g.: identifying a terrorist in a busy Airport terminal

IV. FACE RECOGNITION THE FACE-UNIQUE PART

1. History:
In 1960s, the first semi-automated system for facial recognition to locate the features(such as eyes, ears, nose and mouth) on the photographs. In 1970s, Goldstein and Harmon used 21 specific subjective markers such as hair colour and lip thickness to automate the recognition. I 1988, Kirby and Sirovich used standard linear algebr technique, to the face recognition

2. Facial Recognition:
For face recognition there are two types of comparisons
2.1 Verification: This is where the system compares the given individual with who that individual says they are and gives a yes or no decision.

2.2 Identification: This is where the system compares the given individual to all the other individuals in the database and gives a ranked list of matches.

All identification or authentication technologies operat using the following four stages:
2.2.1 Capture: A physical or behavioural sample is captured by the system during Enrollment and also in identification or verificationa process
2.2.2 Extraction: Unique data is extracted from the sample and a template is created.
2.2.3 Comparison: The template is then compared with a new sample.
2.2.4 Match/Non Match: The system decides if the features extracted from the new Samples are a match or a non match

3. Components of Face Recognition Systems:
3.1 Enrollment Module: An automated mechanism that scans and captures a digital or an analog image of a living personal characteristics.
3.2 Database: Another entity which handles compression, processing, storage and compression of the captured data with stored data.
3.3 Identification Module: The third interfaces with the application system.

4. 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

4.1 Data Acquisition: The input can be recorded video of the speaker or a still image. A sample of 1 sec duration consists of a 25 frame video sequence. More than one camera can be used to produce a 3D representation of the face and to protect against the usage of photographs to gain unauthorized access.

4.2 Input Processing: A pre-processing module locates the eye position and takes care of the surrounding lighting condition and colour variance. First the presence of faces or face in a scene must be detected. Once the face is detected, it must be localized.

Some facial recognition approaches use the whole face while others concentrate on facial components and/ or regions (such as lips, eyes etc). The appearance of the face can change considerably during speech and due to facial expressions.

5. Problem Formulation:

5.1 Occlusion: Occlusion is the state of being obstructed. In the face recognition context, it involves that some parts of the face can't be obtained. For example, a face photograph taken from a surveillance camera could be partially hidden behind a column.

The recognition process can rely heavily on the availability of a full input face. Therefore, the absence of some parts of the face may lead to a bad classification. There are also objects that can occlude facial features glasses, hats, masks, beards, certain hair cuts, etc.

5.2 Optical Technology: A face recognition system should be aware of the format in which the input images are provided. There are different cameras, with different features, different weaknesses and problems.

5.3 Expression Facial: Expression is another variability provider. However, it isn't as strong as illumination or pose. But, the addition of expression variability to pose and illumination problems can become a real impediment for accurate face recognition.

5.4 Algorithm Evaluation: It's not easy to evaluate the effectiveness of a recognition algorithm. Several core factors are unavoidable:

- Error Rate
- Computational Speed
- Memory Usage.

5.5 Illumination: Many algorithms rely on color information to recognize faces. Features are extracted from color images, although some of them may be gray-scale. The color that we perceive from a given surface depends not only on the surface's nature, but also on the light upon it. There can be relevant illumination variations on images taken under uncontrolled environment. The intensity of the color in a pixel can vary greatly depending on the lighting conditions.

As many feature extraction methods relay on color/intensity variability measures between pixels to obtain relevant data, they show an important dependency on lighting changes. Keep in mind that, not only light sources can vary, but also light intensities may increase or decrease, new light sources added. Entire face regions be obscured or in shadow, and also feature extraction can become impossible because of solarization.

The big problem is that two faces of the same subject but with illumination variations may show more differences between them than compared to another subject. Summing up, illumination is one of the big challenges of automated face recognition systems.

5.6 Pose/View Point: The images of a face vary because of the relative cameraface pose (frontal, 45°, profile , upside down) , and some facial features such as the eyes or nose may become partially or wholly occluded.

In fact, pose changes affect the recognition process because of introducing projective deformations and self-occlusion. Thus, pose-tolerance becomes even more critical for face recognition systems that rely on a single view of a subject.

5.7 Ageing and Wrinkles: Ageing can be natural (because of age progression) and artificial (using makeup tools). In both cases,ageing and wrinkles can severely affect the performance of face recognition methods. In general, the effect of age variation or age factor is not commonly considered in face recognition research.

One of the main reasons for the small number of studies concerning face recognition realised in the context of age factor is the absence of representative public databases with images containing individuals of different ages as well as the low quality of old images as documented in the literature. As it is very difficult to collect a dataset for face images that contains images for the same person taken at different ages along his/her life.

5.8 Cybersecurity Issues:

Software applications or equipment that may be accessed wireless may result in an increased risk of a data breach. Also, smart-devices and computer controlled equipment to manage or perform the bulk of their operations and workflow can often become an inviting target.

6. Face image classification and decision making:

Facial recognition software is based on the ability to first recognize faces, which is a technological feat in itself. If you look at 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.

Synergetic computer are used to classify optical and audio features, respectively. A synergetic computer is a set of algorithm that simulate synergetic phenomena. In training phase the BIOID creates a prototype called face print for each person. A newly recorded pattern is pre-processed and compared with each face print stored in the database. As comparisons are made, the system assigns a value to the comparison using a scale of one to ten. If a score is above a predetermined threshold, a match is declared.

If you look at 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. Software defines these landmarks as nodal points.

There are about "80 nodal points" on a human face. Here are few nodal points that are measured by the software:

- Distance between the eyes
- Width of the nose
- Depth of the eye socket
- Cheekbones
- Jaw Line
- Chin

6.1 Face Bunch Graph: A Face bunch graph is created from "70 nodal points" to obtain a general representation of face. Given an image the face is matched to the Face bunch graph to find the same point.These nodal points are measured to create a numerical code, a string of numbers that represents a face in the database. This code is called face print.Only 14 to 22 nodal points are needed for face it software to complete the recognition process.

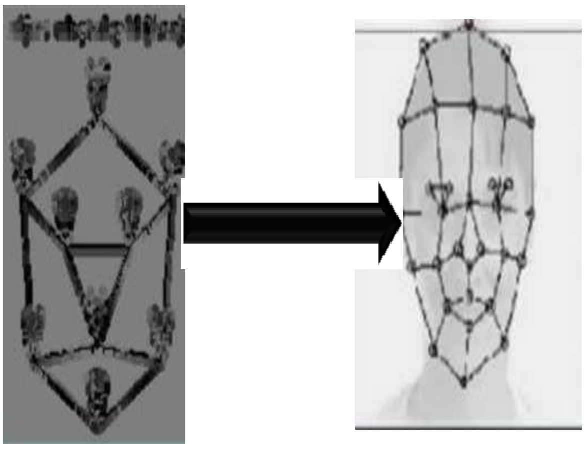


Fig 1. Nodal points are measured to create a numerical code.

6.2 Eigen Faces Algorithm: The major approaches used for face recognition:

- Featured Based Approach
- Eigenface Based Approach

Eigenfaces refers to an appearance-based approach to face recognition that seeks to capture the variation in a collection of face images and use this information to encode and compare images of individual faces in a holistic (as opposed to a parts-based or feature-based) manner.

Specifically, the eigenfaces are the principal components of a distribution of faces, or equivalently, the eigenvectors of the covariance matrix of the set of face images, where an image with N pixels is considered a point (or vector) in N-dimensional space.

The idea of using principal components to represent human faces was developed by Sirovich and Kirby (Sirovich and Kirby 1987) and used by Turk and Pentland (Turk and Pentland 1991) for face detection and recognition.

The Eigenface approach is considered by many to be the first working facial recognition technology, and it served as the basis for one of the top commercial face recognition technology products.

6.2.1 Block Diagram of Face Recognition:

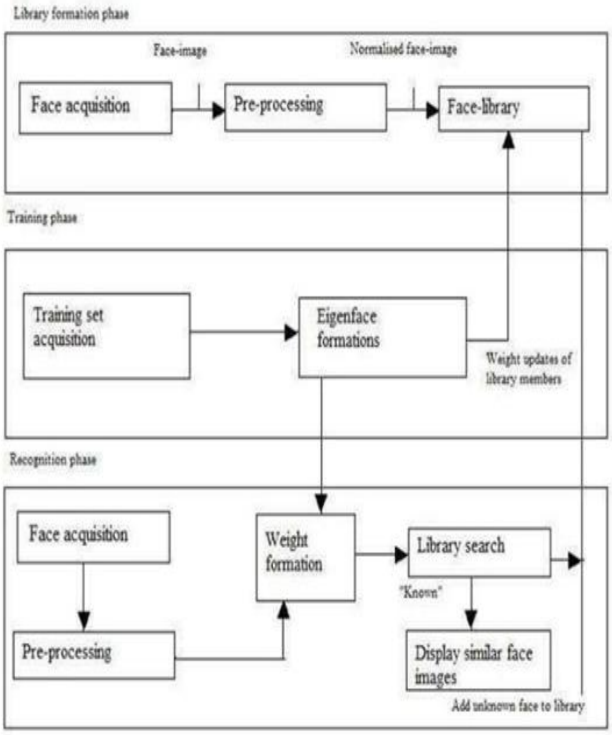


Fig 2. Block Diagram of Face Recognition.

6.2.2 Eigenface Based Facial Algorithm:

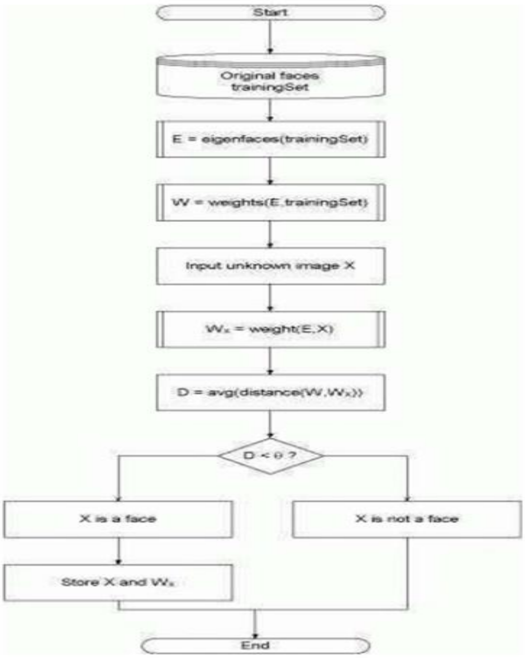
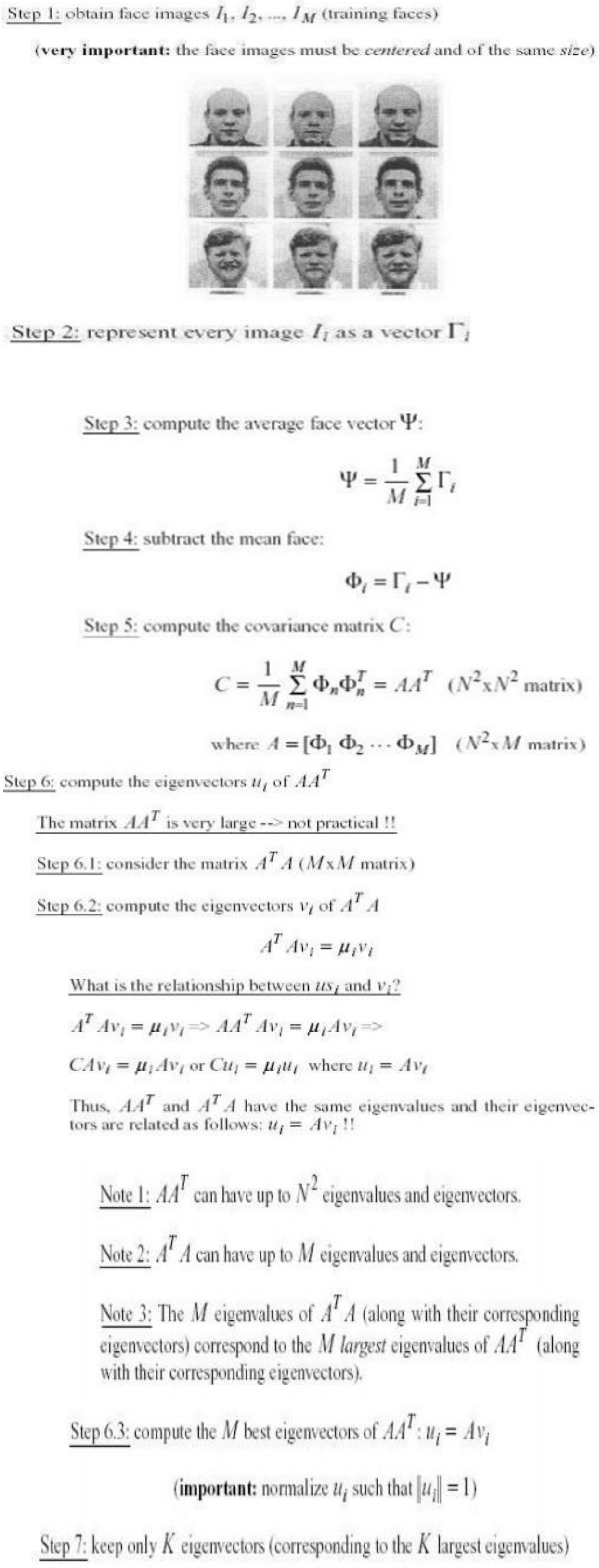


Fig 3. Eigenface Based Facial Algorithm.

6.3 Calculation of eigenfaces with PCA:

In this section, the original scheme for determination ofthe eigenfaces using PCA will be presented. The algorithm described in scope of this paper is a variation of the one outlined here;



Step 1: obtain face images $I_1, I_2, ..., I_M$ (training faces)

(**very important:** the face images must be *centered* and of the same *size*)

Step 2: represent every image I_i as a vector Γ_i

Step 3: compute the average face vector Ψ:

$$\Psi = \frac{1}{M}\sum_{i=1}^{M}\Gamma_i$$

Step 4: subtract the mean face:

$$\Phi_i = \Gamma_i - \Psi$$

Step 5: compute the covariance matrix C:

$$C = \frac{1}{M}\sum_{n=1}^{M}\Phi_n\Phi_n^T = AA^T \quad (N^2 \mathrm{x} N^2 \text{ matrix})$$

where $A = [\Phi_1\ \Phi_2 \cdots \Phi_M]$ (N^2xM matrix)

Step 6: compute the eigenvectors u_i of AA^T

The matrix AA^T is very large --> not practical !!

Step 6.1: consider the matrix A^TA (MxM matrix)

Step 6.2: compute the eigenvectors v_i of A^TA

$$A^TAv_i = \mu_i v_i$$

What is the relationship between us_i and v_i?

$A^TAv_i = \mu_i v_i \Rightarrow AA^TAv_i = \mu_i Av_i \Rightarrow$

$CAv_i = \mu_i Av_i$ or $Cu_i = \mu_i u_i$ where $u_i = Av_i$

Thus, AA^T and A^TA have the same eigenvalues and their eigenvectors are related as follows: $u_i = Av_i$!!

Note 1: AA^T can have up to N^2 eigenvalues and eigenvectors.

Note 2: A^TA can have up to M eigenvalues and eigenvectors.

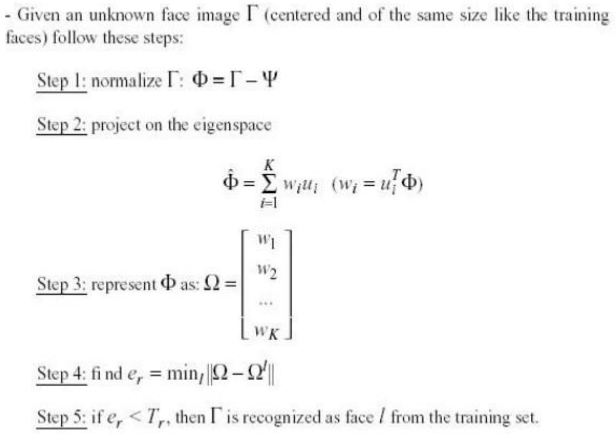
Note 3: The M eigenvalues of A^TA (along with their corresponding eigenvectors) correspond to the M *largest* eigenvalues of AA^T (along with their corresponding eigenvectors).

Step 6.3: compute the M best eigenvectors of AA^T: $u_i = Av_i$

(**important:** normalize u_i such that $\|u_i\| = 1$)

Step 7: keep only K eigenvectors (corresponding to the K largest eigenvalues)

6.4 Face Recognition using EigenFaces:



- Given an unknown face image Γ (centered and of the same size like the training faces) follow these steps:

Step 1: normalize Γ: $\Phi = \Gamma - \Psi$

Step 2: project on the eigenspace

$$\hat{\Phi} = \sum_{i=1}^{K} w_i u_i \quad (w_i = u_i^T \Phi)$$

Step 3: represent Φ as: $\Omega = \begin{bmatrix} w_1 \\ w_2 \\ \dots \\ w_K \end{bmatrix}$

Step 4: fi nd $e_r = \min_l \|\Omega - \Omega^l\|$

Step 5: if $e_r < T_r$, then Γ is recognized as face l from the training set.

V. ADVANTAGES AND DISADVANTAGES

1. Advantages:

- There are many benefits to face recognition systems such as its convince and Social acceptability. all you need is your picture taken for it to work.
- 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.
- It is the only biometric able to operate without user cooperation.
- It can search against static images such as driver's license photographs.
- It has the ability to leverage existing image acquisition equipment.

2. Disadvantages:

- Face recognition systems can't tell the difference between identical twins.
- Changes in acquisition environment
- Changes in physiological characteristics reduce matching accuracy.
- It has the potential for privacy abuse due to noncooperative enrollment and identification capabilities.

VI. APPLICATIONS

The natural use of face recognition technology is the replacement of PIN.

1. Government Use:

1.1 Law Enforcement: Minimizing victim trauma verifying Identify for court records, and comparing school surveillance camera images to know child molesters.

1.2 Security/Counter Terrorism: Access control, comparing surveillance images to Know terrorist.

1.3 Immigration: Rapid progression through Customs.

1.4 Voter Verification: Where eligible politicians are required to verify their identity during a voting process this is intended to stop "proxy" voting where the vote may not go as expected.

2. Commercial Use:

2.1 Residential Security: Alert homeowners of approaching personnel.

2.2 Banking using ATM: The software is able to quickly verify a customer's face.

2.3 Physical access control of buildings areas, doors, cars or net access.

2.4 Voter Verification: Where eligible politicians are required to verify their identity during a voting process this is intended to stop voting where the vote may not go as expected.

2.5 Security/Counterterrorism: Access control, comparing surveillance images to Know terrorist.

VII. CONCLUSION

Face recognition technologies have been associated generally with very costly top secure applications. Today the core technologies have evolved and the cost of equipments is going down dramatically due to the intergration and the increasing processing power. Factors such as environmental changes and mild changes in appearance impact the technology to a greater degree than many expect.

For implementations where the biometric system must verify and identify users reliably over time, facial scan can be a very difficult, but not impossible, technology to implement successfully.Certain applications of face recognition technology are now cost effective, reliable and highly accurate. As a result there are no technological or financial barriers for stepping from the pilot project to widespread deployment.

REFERENCES

[1] Electronics for You: - Part 1 April 2001

[2] Electronics World: - December 2002

[3] www.biometricgroup.com/wiley.

[4] Biometrics- identify verification in a networked world by Samir Nanavati, Micheal Thieme and Raj Nanavati.

[5] History- www.biometrics.gov.

[6] www.facereg.com

[7] www.Imagestechnology.com

[8] www.ieee.com

[9] Intelligent Biometric Techniques in Fingerprint and Face Recognition 1999, by I. Hayashi, Lakhmi C. Jain, S.B. Lee, Shigeyoshi Tsutsui, Ugur Halici.

[10] Face Recognition from Theory to Applictions 2012, by Francoise Fogelman Soulie, Harry Wechsler, Jonathon P. Phillips, Thomas S. Huang, Vicki Bruce.

[11] Face Recognition Semisupervised Classification, Subspace Projection and Evaluation Methods 2016, by S. Ramakrishnan.

[12] Face Recognition: A Literature Review January 2005 By Ahmad TolbaMansoura University, Ali El-Baz Damietta University.

[13] Face Recognition: A Literature Review A.S. Tolba, A.H. El-Baz, and A.A. El-Harby.