CHAPTER – 2
INTRODUCTION TO FINGERPRINT AND FACE RECOGNITION

2.1 Fingerprint recognition

Fingerprint recognition (identification) is one of the oldest methods of identification with biometric traits. Large no. of archeological artifacts and historical items shows the signs of fingerprints of human on stones. The ancient people were aware about the individuality of fingerprint, but they were not aware of scientific methods of finding individuality.

2.1.1 History of Fingerprint recognition

Let us have a look at history fingerprint recognition [2].

2,000 B.C. - Babylonians require fingerprints on contracts to help avoid forgery.

250 B.C. - Chinese officials use fingerprints to seal official documents.

700 A.D. - The Japanese adopt the Chinese practice of signing contracts with fingerprints.

1684 A.D. – England's Nehemiah Grew uses a microscope to study and then publishes the first scientific paper describing the ridges found on fingers and palms.

1788 – German anatomist Johann Christoph Andreas Mayer is the first to recognize that each set of fingerprints is unique.

He wrote: “Although the arrangement of skin ridges is never duplicated in two persons, nevertheless the similarities are closer among some individuals. In others the differences are marked, yet in spite of their peculiarities of arrangement, all have a certain likeness.”.

1880 – Working in Tokyo, surgeon Henry Faulds publishes an article in the journal Nature describing a system for recording fingerprints using ink and using them for criminal identification. Six years later, he takes his idea to London's Metropolitan Police, where it is summarily rejected.

1892 – Argentinean police chief Juan Vucetich establishes the world's first fingerprint bureau to aid in criminal identification and prosecution.

1892 – Galton develops a classification system for fingerprints

1986 – Henry develops a fingerprint classification system
1897 – In Calcutta, India, Officers Azizul Haque and Hem Chandra Bose develop the "Henry System" for fingerprint classification (named after their supervisor, Sir Edward Richard Henry).

1898 – The first case in which fingerprints are used to obtain a criminal conviction takes place in Bengal, India.

1901 – The Henry System is adopted by Scotland Yard.

1903 – NY state prisons begin using fingerprints.

1906 – Fingerprinting is adopted as an investigative tool by the New York City Police Department.

1911 – In the case of People v. Jennings, a U.S. Court of Appeals rules favorably on the admissibility of fingerprints as evidence in criminal cases. A person v. Crispi is the first criminal conviction obtained solely on fingerprint evidence.

1969 – FBI pushes to make fingerprint recognition an automated process

1975 – FBI funds development of sensors and minutiae extracting technology

1981 – Five AFIS deployed

1986 – Exchange of fingerprint minutiae data standard published

1994 – IAFIS competition organized.

1999 – IAFIS components put in to operation

After this, commercial products of fingerprint verification became popular in the market for various access control, log on and verification functions.

2.1.2 Working of fingerprint recognition

The working of fingerprint verification and identification is similar in mostly all vendors.

Typical fingerprint verification process involves five stages [3]:

- Fingerprint image acquisition
- Image processing
- Location of distinctive characteristics
- Template creation
- Template matching

1. Fingerprint image acquisition
The first challenge facing a finger-scan system is to acquire a high-quality image of the fingerprint. Image quality is measured in dots per inch (DPI) - more dots per inch means a higher-resolution image. Today’s finger-scan peripherals can acquire images of 500 DPI, the standard for forensic-quality fingerprinting. The lowest DPI generally found in the market is in the 250- to 300-DPI range. Example fingerprint with different DPI is shown in figure 2.1.

Image acquisition is a major challenge for finger-scan developers, because fingerprint quality can vary substantially from person to person and from finger to finger. Some populations are more likely than others to have faint or difficult-to-acquire fingerprints, whether due to wear and tear or physiological traits. In addition, environmental factors can impact image acquisition. In very cold weather, the oils normally found on a fingerprint (which make for better imaging) dry up, such that fingerprints can appear faint. Users may need to press more firmly or even rub the finger into their opposite palm to ensure that a quality image is acquired.

For a finger-scan image to act as an effective enrollment, the center of the fingerprint must be placed on the platen. Many users unfamiliar with the technology will place their finger at an angle, such that only the upper portion of the fingerprint appears. This results in fewer distinctive features being located during enrollment and verification, reducing the likelihood of successful operation.

An additional factor in image acquisition that can affect a system’s accuracy and performance is the size of the platen. Over time, finger-scan vendors have developed smaller and smaller platens in order to manufacture smaller devices and to reduce costs. However, there may be a point of diminishing returns in terms of minimizing platen size. Very small platens acquire a smaller portion of the fingerprint, meaning that less data is available to create and match templates. Users with large fingers may also find it difficult to present their fingerprint in a consistent fashion, leading to false rejections.
2. Image processing

Once a high-quality image is acquired, it must be converted to a usable format. Image processing subroutines eliminate gray areas from the image by converting the fingerprint image’s gray pixels to white and black, depending on their pitch. What results is a series of thick black ridges (the raised part of the fingerprint) contrasted to white valleys. The ridges are then thinned from approximately 5 to 8 pixels in width down to a single pixel, for precise location of features (figure 2.4).
3. Location of Distinctive Characteristics
The fingerprint comprises ridges and valleys that form distinctive patterns, such as swirls, loops, and arches. Most fingerprints also have a core, a central point around which swirls, loops, or arches are curved. Deltas are points, normally at the lower left or right corner of the fingerprint, around which ridges are centered in a triangular shape.
Fingerprint ridges and valleys are characterized by discontinuities and irregularities known as minutiae—these are the distinctive features on which most finger-scan technologies are based. There are many types of minutiae, the most common being ridge endings (the point at which a ridge ends) and bifurcations (the point at which one ridge divides into two). Depending on the size of the platen and the quality of the vendor algorithm, a typical finger-scan image may produce between 15 and 50 minutiae—larger platens will acquire more of the fingerprint image, meaning that a greater number of minutiae can be located. Figure 2.5 shows typical fingerprint with different minutiae points.
4. Template creation

Vendors utilize proprietary algorithms to map fingerprint minutiae. Information used when mapping minutiae can include the location and angle of a minutia point, the type and quality of minutiae, and the distance and position of minutiae relative to the core. A user normally must place his or her enrollment fingerprint more than once during enrollment, so that the system can locate the most consistently generated minutiae.

Finger-scan images will normally have distortions and false minutiae that must be filtered out before template creation. For example, anomalies caused by scars, sweat, or dirt can appear as minutiae. Vendor algorithms scan images and eliminate features that simply seem to be in the wrong place, such as adjacent minutiae or a ridge crossing perpendicular to a series of other ridges. A large percentage of false minutiae are discarded in this process, ensuring that the template generated for enrollment or verification is an accurate reflection of the biometric data.

5. Template matching

Finger-scan templates can range in size from approximately 200 bytes to over 1,000 bytes—a very small amount of data by any measure. These templates cannot be manually read as anything resembling a fingerprint, and simply performing a bit-to-bit comparison of two finger-scan templates will not determine whether they are from the same person. Instead, vendor algorithms are required to process templates and to determine the correlation between the two.

Comparing enrollment and verification templates does not result in an exact match. The position of a minutia point may change by a few pixels, some minutiae will differ from the enrollment template, and false minutiae may be seen as real. Also, the fingerprint will inevitably be placed at a slightly different angle. However, matching algorithms can account for these variations and allow for effective comparison of templates in which much of the underlying data may have changed.

There is no minimum number of minutiae necessary for two finger-scan templates to match. In some cases, the system may need to locate only a handful of minutiae in common to decide that two templates are a match. Higher system thresholds will require that a higher percentage of the minutiae points match and can require more careful placement during verification. If a fingerscan is deployed for 1:few identification against
modest databases as opposed to 1:1 verification, these thresholds will likely need to be increased. The most basic determinant of these thresholds will be whether the system is implemented for convenience or security.

2.1.3 Scanners for fingerprint recognition

The quality of the fingerprint image must be good enough to create template. There are number of methods for scanning fingerprint image. The leading technologies are: Optical, Silicon and Ultrasound.

Optical technology is the oldest and most widely used. The finger is placed on a coated platen, usually built of hard plastic but proprietary to each company. In most devices, a charged coupled device (CCD) converts the image of the fingerprint, with dark ridges and light valleys, into a digital signal. The brightness is either adjusted automatically (preferable) or manually (difficult), leading to a usable image.

Optical devices have several strengths: they are the most proven over time; they can withstand, to some degree, temperature fluctuations; they are fairly inexpensive; and they can provide resolutions up to 500 dpi. Drawbacks to the technology include size - the platen must be of sufficient size to achieve a quality image - and latent prints. Latent prints are leftover prints from previous users. This can cause image degradation, as severe latent prints can cause two sets of prints to be superimposed. Also, the coating and CCD arrays can wear with age, reducing accuracy.

Optical is the most implemented technology by a significant margin. Identicator and its parent company Identix, two of the most prominent fingerprint companies, utilize optical technology, much of which is developed jointly with Motorola. The majority of companies use optical technology, but and increasing number of vendors utilize silicon technology.

Silicon technology has gained considerable acceptance since its introduction in the late 90's. Most silicon, or chip, technology is based on DC capacitance. The silicon sensor acts as one plate of a capacitor, and the finger is the other. The capacitance between platen and the finger is converted into an 8-bit grayscale digital image. With the exception of AuthenTec, whose technology employs AC capacitance and reads to the live layer of skin, all silicon fingerprint vendors use a variation of this type of capacitance.
Silicon generally produces better image quality, with less surface area, than optical. Since the chip is comprised of discreet rows and columns - between 200-300 lines in each direction on a 1cmx1.5cm wafer - it can return exceptionally detailed data. The reduced size of the chip means that costs should drop significantly, now that much of the R&D necessary to develop the technology is bearing fruit. Silicon chips are small enough to be integrated into many devices which cannot accommodate optical technology. 

Silicon's durability, especially in sub-optimal conditions, has yet to be proven. Although manufacturers use coating devices to treat the silicon, and claim that the surface is 100x more durable than optical, this has to be proven. Also, with the reduction in sensor size, it is even more important to ensure that enrolment and verification are done carefully - a poor enrollment may not capture the center of the fingerprint, and subsequent verifications are subject to the same type of placement. Many major companies have recently moved into the silicon field. Infineon (the semiconductor division of Siemens) and Sony have developed chips to compete with Veridicom (a spin-off of Lucent), the leader in silicon technology.

Ultrasound technology, though considered perhaps the most accurate of the fingerprint technologies, is not yet widely used. It transmits acoustic waves and measures the distance based on the impedance of the finger, the platen, and air. Ultrasound is capable of penetrating dirt and residue on the platen and the finger, countering a main drawback to optical technology.

Until ultrasound technology gains more widespread usage, it will be difficult to assess its long-term performance. However, preliminary usage of products from Ultra-Scan Corporation (USC) indicates that this is a technology with significant promise. It combines strength of optical technology, large platen size and ease of use, with strength of silicon technology, the ability to overcome sub-optimal reading conditions.

2.1.4 Fingerprint classification

Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, access control, and driver license registration. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database. To reduce the search time
and computational complexity, it is desirable to classify these fingerprints in an accurate
and consistent manner so that the input fingerprint is required to be matched only with a
subset of the fingerprints in the database.

Fingerprint classification is a technique to assign a fingerprint into one of the several pre-
specified types already established in the literature which can provide an indexing
mechanism. Fingerprint classification can be viewed as a coarse level matching of the
fingerprints. An input fingerprint is first matched at a coarse level to one of the pre-
specified types and then, at a finer level, it is compared to the subset of the database
containing that type of fingerprints only. An algorithm is developed to classify
fingerprints into five classes, namely, whorl, right loop, left loop, arch, and tented arch.
The algorithm separates the number of ridges present in four directions (0 degree, 45
degree, 90 degree, and 135 degree) by filtering the central part of a fingerprint with a
bank of Gabor filters. This information is quantized to generate a FingerCode which is
used for classification. Our classification is based on a two-stage classifier which uses a
K-nearest neighbor classifier in the first stage and a set of neural networks in the second
stage. The classifier is tested on 4,000 images in the NIST-4 database. For the five-class
problem, classification accuracy of 90% is achieved. For the four-class problem (arch and
tented arch combined into one class), we are able to achieve a classification accuracy of
94.8%. By incorporating a reject option, the classification accuracy can be increased to
96% for the five-class classification and to 97.8% for the four-class classification when
30.8% of the images are rejected. Classification is shown in figure 2.6.

2.1.5 Fingerprint feature extraction
The human fingerprint is comprised of various types of ridge patterns, traditionally
classified according to the decades-old Henry system: left loop, right loop, arch, whorl,
and tented arch. Loops make up nearly 2/3 of all fingerprints, whorls are nearly 1/3, and
perhaps 5-10% is arches. These classifications are relevant in many large-scale forensic
applications, but are rarely used in biometric authentication.

Minutiae (Figure 2.5), the discontinuities that interrupt the otherwise smooth flow of
ridges, are the basis for most fingerprint authentication. Codified in the late 1800’s as
Galton features, minutiae are at their most rudimentary ridge endings, the points at which
a ridge stops, and bifurcations, the point at which one ridge divides into two. Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other).

![Figure 2.6 Classification of fingerprints – a. Left loop b. Right loop c. Whorl d. Arch e. Tented arch](image)

Other features are essential to fingerprint authentication. The core is the inner point, normally in the middle of the print, around which swirls, loops, or arches center. It is frequently characterized by a ridge ending and several acutely curved ridges. Deltas are the points, normally at the lower left and right hand of the fingerprint, around which a triangular series of ridges center.

The ridges are also marked by pores, which appear at steady intervals. Some initial attempts have been made to use the location and distribution of the pores as a means of authentication, but the resolution required to capture pores consistently is very high.

Once a high-quality image is captured, there are several steps required to convert its distinctive features into a compact template. This process, known as feature extraction, is at the core of fingerprint technology. Each of the 50 primary fingerprint vendors has a
proprietary feature extraction mechanism; the vendors guard these unique algorithms very closely. What follows is a series of steps used, in some fashion, by many vendors - the basic principles apply even to those vendors who use alternative mechanisms.

The image must then be converted to a usable format. If the image is grayscale, areas lighter than a particular threshold are discarded, and those darker are made black. The ridges are then thinned from 5-8 pixels in width down to one pixel, for precise location of endings and bifurcations.

Minutiae localization begins with this processed image. At this point, even a very precise image will have distortions and false minutiae that need to be filtered out. For example, an algorithm may search the image and eliminate one of two adjacent minutiae, as minutiae are very rarely adjacent. Anomalies caused by scars, sweat, or dirt appear as false minutiae, and algorithms locate any points or patterns that don't make sense, such as a spur on an island (probably false) or a ridge crossing perpendicular to 2-3 others (probably a scar or dirt). A large percentage of would-be minutiae are discarded in this process.

The point at which a ridge ends, and the point where a bifurcation begins, are the most rudimentary minutiae, and are used in most applications. There is variance in how exactly to situate a minutia point: whether to place it directly on the end of the ridge, one pixel away from the ending, or one pixel within the ridge ending (the same applies to bifurcation). Once the point has been situated, its location is commonly indicated by the distance from the core, with the core serving as the 0,0 on an X,Y-axis. Some vendors use the far left and bottom boundaries of the image as the axes, correcting for misplacement by locating and adjusting from the core. In addition to the placement of the minutia, the angle of the minutia is normally used. When a ridge ends, its direction at the point of termination establishes the angle (more complicated rules can apply to curved endings). This angle is taken from a horizontal line extending rightward from the core, and can be up to 359.

In addition to using the location and angle of minutiae, some vendors classify minutia by type and quality. The advantage of this is that searches can be quicker, as a particularly notable minutia may be distinctive enough to lead to a match. A vendor can also rank high versus low quality minutia and discard the latter. Those vendors who shy away from
this methodology do so because of the wide variation from print to print, even on successive submissions. Measuring quality may only introduce an unnecessary level of complication.

Approximately 80% of biometric vendors utilize minutiae in some fashion. Those who do not utilize minutia use pattern matching, which extrapolates data from a particular series of ridges. This series of ridges used in enrollment is the basis of comparison, and verification requires that a segment of the same area be found and compared. The use of multiple ridges reduces dependence on minutiae points, which tend to be affected by wear and tear. The templates created in pattern matching are generally, but not always, 2-3 times larger than in minutia - usually 900-1200 bytes.

2.1.6 Fingerprint matching

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation. Here are three matching techniques which can be used for fingerprint recognition [1].

- Correlation based matching: two fingerprint images are superimposed and the correlation (at the intensity level) between corresponding pixels is computed for different alignments (e.g., various displacements and rotations);
- Minutiae based matching: minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. A minutia matching essentially consists of finding the alignment between the template and the input minutiae set that results in the maximum number of minutiae pairings;
- Ridge feature-based matching: minutiae extraction is difficult in very low-quality fingerprint images, whereas other features of the fingerprint ridge pattern (e.g., local
orientation and frequency, ridge shape, texture information) may be extracted more reliably than minutiae, even though their distinctiveness is generally lower. The approaches belonging to this family compare fingerprints in term of features extracted from the ridge pattern.

2.1.7 Strengths and weaknesses of fingerprint recognition

1. Strengths
   - Proven technology capable of high levels of accuracy
   - Range of deployment environments
   - Ergonomic easy to use devices
   - Ability to enroll multiple fingers

2. Weaknesses
   - Inability to enroll some users
   - Performance deterioration over time
   - Association with forensic applications
   - Need to deploy specialized devices

2.1.8 Application domains of fingerprint recognition

Applications of fingerprint recognition can be divided into three categories: Forensic applications, government applications, Commercial applications. The following table describes overall view of applications of fingerprint recognition.

<table>
<thead>
<tr>
<th>Forensic applications</th>
<th>Government applications</th>
<th>Commercial applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corpse identification</td>
<td>National ID card</td>
<td>Computer network logon</td>
</tr>
<tr>
<td>Criminal investigation</td>
<td>Correctional facility</td>
<td>Electronic data security</td>
</tr>
<tr>
<td>Terrorist identification</td>
<td>Driver’s license</td>
<td>E-commerce</td>
</tr>
<tr>
<td>Parenthood determination</td>
<td>Social security</td>
<td>Internet access</td>
</tr>
<tr>
<td>Missing children</td>
<td>Welfare disbursement</td>
<td>ATM, credit card</td>
</tr>
<tr>
<td></td>
<td>Border control</td>
<td>Physical access control</td>
</tr>
<tr>
<td></td>
<td>Passport control</td>
<td>Cellular phones</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PDAs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medical record management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distance learning</td>
</tr>
</tbody>
</table>

Table – 2.1 Fingerprint recognition applications
2.1.9 Factors affecting success rate of fingerprint recognition

The following conditions affect the success rate of fingerprint recognition systems:

- Cold finger
- Dry/oily finger
- High or low humidity
- Angle of placement
- Pressure of placement
- Location of finger on platen (poorly placed core)
- Cuts to fingerprint
- Manual activity that would mar or affect fingerprints (construction, gardening)

2.2 Face recognition

A smart environment is one that is able to identify people, interpret their actions, and react appropriately. Thus, one of the most important building blocks of smart environments is a person identification system. Face recognition devices are ideal for such systems, since they have recently become fast, cheap, unobtrusive, and, when combined with voice-recognition, are very robust against changes in the environment. Moreover, since humans primarily recognize each other by their faces and voices, they feel comfortable interacting with an environment that does the same.

Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. The programs take a facial image, measure characteristics such as the distance between the eyes, the length of the nose, and the angle of the jaw, and create a unique file called a "template." Using templates, the software then compares that image with another image and produces a score that measures how similar the images are to each other.

2.2.1 History of Face recognition

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.
Developed in the 1960s, the first semi-automated system for face recognition required the administrator to locate features (such as eyes, ears, nose, and mouth) on the photographs before it calculated distances and ratios to a common reference point, which were then compared to reference data. In the 1970s, Goldstein, Harmon, and Lesk used 21 specific subjective markers such as hair color and lip thickness to automate the recognition. The problem with both of these early solutions was that the measurements and locations were manually computed. In 1988, Kirby and Sirovich applied principle component analysis, a standard linear algebra technique, to the face recognition problem. This was considered somewhat of a milestone as it showed that less than one hundred values were required to accurately code a suitably aligned and normalized face image. In 1991, Turk and Pentland discovered that while using the eigenfaces techniques, the residual error could be used to detect faces in images – a discovery that enabled reliable real-time automated face recognition systems. Although the approach was somewhat constrained by environmental factors, it nonetheless created significant interest in furthering development of automated face recognition technologies. The technology first captured the public’s attention from the media reaction to a trial implementation at the January 2001 Super Bowl, which captured surveillance images and compared them to a database of digital mugshots. This demonstration initiated much-needed analysis on how to use the technology to support national needs while being considerate of the public’s social and privacy concerns. Today, face recognition technology is being used to combat passport fraud, support law enforcement, identify missing children, and minimize benefit/identity fraud.

### 2.2.2 Working of Face recognition

Facial technology follows the same procedure of biometric procedure: image acquisition, image processing, distinctive characteristic location, template creation and matching [3].

1. **Image acquisition**

Facial-scan technology can acquire faces from almost any static camera or video system that generates images of sufficient quality and resolution. Ideally, images acquired for facial-scan will be acquired through high-resolution cameras, with users directly facing the camera and with moderate lighting of the face. High-quality enrollment is essential to
eventual verification and identification; enrollment images define the facial characteristics to be used in all future authentication events. Although certain technologies can search digitized images for faces as small as 30 pixels in height, the technology performs much better when the height and width of the facial images each exceeds 100 pixels.

Image acquisition becomes more difficult and the technology’s accuracy becomes less robust under many circumstances. Distance from camera reduces facial size and therefore image resolution, though the technology is capable of magnifying smaller faces to increase the possibility of template generation. Users not looking directly at the camera—positioned more than approximately 15 degrees—either vertically or horizontally, away from ideal positioning—are less likely to have images acquired by some technologies. There is also a gap between the threshold for locating faces in a field of view and locating usable faces—a system may be able to locate a face from a sharp angle, but be unable to subsequently enroll or identify the individual from this image. To overcome the acquisition-angle problem, newer facial-scan methods actually require that the user look left, right, up, and down in order to acquire images from various angles, thus building a more comprehensive enrollment template.

While angled acquisition is being addressed in certain facial-scan technologies, the problem of lighting is more severe. While the human brain is capable of acquiring facial images under drastically different lighting conditions, facial scan technologies are generally unable to acquire images that are somewhat overexposed or underexposed. Systems with automatic gain control, able to adjust for different lighting conditions and skin tone, are more likely to present images from which facial-scan solutions can acquire faces. Facial-scan systems’ sensitivity to lighting and gain can actually result in reduced ability to acquire faces from individuals of certain races and ethnicities. Select Hispanic, Black, and Asian individuals can be more difficult to enroll and verify in some facial-scan systems because acquisition devices are not always optimized to acquire darker faces. At times, an individual may stand in front of a facial-scan system and simply not be found. While the issue of failure-to-enroll is present in all biometric systems, many are surprised that facial-scan systems occasionally encounter faces they cannot enroll.
The severity of these image acquisition challenges applies in varying degrees to facial-scan systems implemented for 1:1 verification, for 1:N public-sector identification, and for surveillance. Generally speaking, 1:N public-sector identification systems are most likely to have controlled and consistent enrollment environments: Users can be required to stand at a fixed distance from a camera, with fixed lighting and a fixed background. In 1:1 verification, variables such as changes in lighting and acquisition angle are likely to be introduced, and the lack of supervision in most 1:1 verification implementations exacerbates the problem. Surveillance is a worst-case scenario as images are acquired from unaware subjects, moving at various speeds and angles, through cameras that generally lack active gain control. Because initial image acquisition is critical to system operations, deployers must be sure to take every variable into account when determining how and where to implement facial-scan technology.

2. Image processing
After completing image acquisition procedure, image processing follows. Images are cropped such that the ovoid facial image remains, and color images are normally converted to black and white in order to facilitate initial comparisons based on grayscale characteristics. Facial images are then normalized to overcome variations in orientation and distance. In order to do this, basic characteristics such as the middle of the eyes are located and used as a frame of reference. Once the eyes are located, the facial image can be rotated clockwise or counterclockwise to straighten the image along a horizontal axis. The face can then be magnified, if necessary, so that the facial image occupies a minimum pixel space. Since most facial-scan systems acquire multiple face images to enroll individuals—from as few as 3 images to well over 100, depending on the vendor and the matching method—rapid image processing routines are essential to system operations.

3. Distinctive characteristics
After standardizing the image as per requirement of vendor, next step to the core process, which identifies distinctive characteristic locations. While there are various matching methods, all facial-scan systems attempt to match visible facial features in a fashion similar to the way people recognize one another. The features most often utilized in facial-scan systems are those least likely to change significantly over time: upper ridges
of the eye sockets, areas around the cheekbones, sides of the mouth, nose shape, and the position of major features relative to each other. Areas which are very likely to change or to be obscured, such as areas of the face immediately adjacent to a hairline, are usually not relied upon for verification. See the section entitled Competing Facial-Scan Technologies for discussion of the leading facial-scan methodologies.

One of the challenges involved in facial-scan technology is that the face is a reasonably changeable physiological characteristic. As opposed to a fingerprint, which might be scarred but is difficult to alter dramatically, faces can be changed enough to reduce a system’s matching accuracy. A user, who smiles during enrollment and grimaces during verification or identification, is more likely to be rejected than one, who does not intentionally alter his or her expression during authentication. Behavioral changes such as alteration of hairstyle, changes in makeup, growing or shaving facial hair, adding or removing eyeglasses are behaviors that impact the ability of facial-scan systems to locate distinctive features. While the human brain may be able to account for many of these changes, facial-scan systems are not yet developed to the point where they can overcome such variables.

4. Template creation

Enrollment templates are normally created from a multiplicity of processed facial images. These templates can vary in size from less than 100 bytes, generated through certain vendors’ quick-search algorithms, to over 3K for templates created through full search algorithms. These templates cannot be used to recreate original images, but are instead proprietary representations of the data located during feature location. The 3K template is by far the largest among technologies considered physiological biometrics. Larger templates are normally associated with behavioral biometrics, wherein it is difficult to locate distinctive characteristics with precision.

5. Template matching

Vendors employ proprietary methods to compare match templates against enrollment templates, assigning confidence levels to the strength of each match attempt. If the score surpasses a predefined level, the comparison is deemed a match. In many cases, a series of images is acquired and scored against the enrollment, so that a user attempting 1:1 verification within a facial-scan system may have 10 to 20 match attempts take place.
within 1 to 2 seconds. This sets facial-scan apart from most other biometrics, in which a single match template is acquired and scored, and, if necessary, the user is prompted to attempt again. Whereas in most 1:1 biometric systems a rejection is defined as a failure to match after a given number of attempts (often 1 to 3), a rejection in a facial-scan system is often defined as a failure to match after a certain amount of time.

In identification, the number of match attempts and the rate of matching will increase dramatically. Leading facial-scan systems can perform tens of thousands of identification comparisons per second through standard PCs. These rapid searches often take place through the smaller template generated in facial-scan systems. Because facial-scan is not as effective as finger-scan or iris-scan in identifying a single individual from a large database, a number of potential matches are generally returned after large-scale facial-scan identification searches. For example, a system may be configured to return the 10 most likely matches on a search of a 10,000-person database. A human operator would then determine which if any of the 10 potential matches an actual match is.

### 2.2.3 Image based face recognition algorithms

Here is the list of image based face recognition algorithms [4].

1. **PCA**
   
   It is derived from Karhunen-Loeve's transformation. Given an s-dimensional vector representation of each face in a training set of images, Principal Component Analysis (PCA) tends to find a t-dimensional subspace whose basis vectors correspond to the maximum variance direction in the original image space. This new subspace is normally lower dimensional (t<<s). If the image elements are considered as random variables, the PCA basis vectors are defined as eigenvectors of the scatter matrix.

2. **ICA**
   
   Independent Component Analysis (ICA) minimizes both second-order and higher-order dependencies in the input data and attempts to find the basis along which the data (when projected onto them) are *statistically independent*. Bartlett et al. provided two architectures of ICA for face recognition task: *Architecture I* - statistically independent basis images, and *Architecture II* - factorial code representation.

3. **LDA**
Linear Discriminant Analysis (LDA) finds the vectors in the underlying space that best discriminate among classes. For all samples of all classes the between-class scatter matrix $S_B$ and the within-class scatter matrix $S_W$ are defined. The goal is to maximize $S_B$ while minimizing $S_W$, in other words, maximize the ratio $\det|S_B|/\det|S_W|$.

This ratio is maximized when the column vectors of the projection matrix are the eigenvectors of $(S_W^{-1} \times S_B)$.

4. EP
An eigenspace-based adaptive approach that searches for the best set of projection axes in order to maximize a fitness function, measuring at the same time the classification accuracy and generalization ability of the system. Because the dimension of the solution space of this problem is too big, it is solved using a specific kind of genetic algorithm called Evolutionary Pursuit (EP).

5. EBGM
Elastic Bunch Graph Matching (EBGM). All human faces share a similar topological structure. Faces are represented as graphs, with nodes positioned at fiducial points (eyes, nose...) and edges labeled with 2-D distance vectors. Each node contains a set of 40 complex Gabor wavelet coefficients at different scales and orientations (phase, amplitude). They are called "jets". Recognition is based on labeled graphs. A labeled graph is a set of nodes connected by edges, nodes are labeled with jets, edges are labeled with distances.

6. Kernel Methods
The face manifold in subspace need not be linear. Kernel methods are a generalization of linear methods. Direct non-linear manifold schemes are explored to learn this non-linear manifold.

7. Trace Transform
The Trace transform, a generalization of the Radon transform, is a new tool for image processing which can be used for recognizing objects under transformations, e.g. rotation, translation and scaling. To produce the Trace transform one computes a functional along tracing lines of an image. Different Trace transforms can be produced from an image using different trace functionals.

8. AAM
An Active Appearance Model (AAM) is an integrated statistical model which combines a model of shape variation with a model of the appearance variations in a shape-normalized frame. An AAM contains a statistical model if the shape and gray-level appearance of the object of interest which can generalize to almost any valid example. Matching to an image involves finding model parameters which minimize the difference between the image and a synthesized model example projected into the image.

9. 3-D Morphable Model
Human face is a surface lying in the 3-D space intrinsically. Therefore the 3-D model should be better for representing faces, especially to handle facial variations, such as pose, illumination etc. Blantz et al. proposed a method based on a 3-D morphable face model that encodes shape and texture in terms of model parameters, and algorithm that recovers these parameters from a single image of a face.

10. 3-D Face Recognition
The main novelty of this approach is the ability to compare surfaces independent of natural deformations resulting from facial expressions. First, the range image and the texture of the face are acquired. Next, the range image is preprocessed by removing certain parts such as hair, which can complicate the recognition process. Finally, a canonical form of the facial surface is computed. Such a representation is insensitive to head orientations and facial expressions, thus significantly simplifying the recognition procedure. The recognition itself is performed on the canonical surfaces.

11. Bayesian Framework
A probabilistic similarity measure based on Bayesian belief that the image intensity differences are characteristic of typical variations in appearance of an individual. Two classes of facial image variations are defined: intrapersonal variations and extrapersonal variations. Similarity among faces is measures using Bayesian rule.

12. SVM
Given a set of points belonging to two classes, a Support Vector Machine (SVM) finds the hyperplane that separates the largest possible fraction of points of the same class on the same side, while maximizing the distance from either class to the hyperplane. PCA is first used to extract features of face images and then discrimination functions between each pair of images are learned by SVMs.
13. HMM

Hidden Markov Models (HMM) are a set of statistical models used to characterize the statistical properties of a signal. HMM consists of two interrelated processes: (1) an underlying, unobservable Markov chain with a finite number of states, a state transition probability matrix and an initial state probability distribution and (2) a set of probability density functions associated with each state.

2.2.4 Other efficient methods of face recognition

Three other suitable methods of recognition are Eigenface, Neural network and Feature analysis. Let us look at these methods.

1. Eigenface

Eigenface, roughly translated as “one’s own face,” is a technology patented at MIT that utilizes a database of two-dimensional, grayscale facial images (Eigenfaces) from which templates are created during enrollment and verification. These Eigenfaces feature distinctive facial characteristics, and the vast majority of faces can be reconstructed by locating distinctive features from approximately 100 to 125 Eigenfaces. Variations of Eigenface are frequently used as the basis of other face-recognition methods.

Upon enrollment, a subject’s facial image is represented using a combination of various Eigenfaces. This reconstruction is then mapped to a series of numbers or coefficients. For 1:1 authentication, in which the image is being used to verify a claimed identity, an individual’s live template is compared against the enrolled template to determine coefficient variation. The degree of variance from the enrollment will determine acceptance or rejection. For 1-to-many identification, the same principle applies, but with a much larger comparison set. Like all facial recognition technology, Eigenface technology is best utilized in well-lit, frontal image capture situations.
Feature analysis is perhaps the most widely utilized facial recognition technology. This technology is related to Eigenface, but is more capable of accommodating changes in appearance or facial aspect (smiling versus frowning, for example). Visionics, a prominent facial recognition company, uses Local Feature Analysis (LFA), which can be summarized as a reduction of facial features to an “irreducible set of building elements.” Feature analysis derives enrollment and verification templates from dozens of features from different regions of the face and also incorporates the relative location of these features. The extracted features are building blocks, and both the type of blocks and their arrangement are used for identification and verification. It anticipates that the slight movement of a feature located near one’s mouth will be accompanied by relatively similar movement of adjacent features. Since feature analysis is not a global representation of the face, it can accommodate angles up to approximately 25 degrees in the horizontal plane, and approximately 15 degrees in the vertical plane. A straight-ahead facial image from a distance of 3 feet will be the most accurate.

3. Neural network
Neural network systems employ algorithms to determine the similarity of the unique global features of live versus enrolled or reference faces, using as much of the facial image as possible. Neural systems are designed to learn which features are most effective within the body of users that the system is intended to serve. Features from both the enrollment and the verification faces vote on whether there is a match. An incorrect vote, such as a false match, prompts the matching algorithm to modify the weight it gives to certain facial features. In this way, neural network systems learn which features are most effective for matching and pragmatically adjust themselves based on the methods that have proven most effective. This method, theoretically, leads to an increased ability to identify faces in difficult conditions.

Other facial technologies have emerged based on more advanced neural models, with detailed cells incorporating thousands of facial images. Since these technologies are capable of learning over time, they may be capable of reducing the time-based performance problems found in many facial-scan systems. However, their elongated enrollment process means that they are not well-suited for surveillance applications in which users are matched against watch lists. These watch lists are often generated from static images, not the ideal environment for neural net enrollment.

### 2.2.5 Applications of Face recognition

One of the reasons face recognition has attracted so much research attention and sustained development over the past 30 years is its great potential in numerous government and commercial applications. In 1997, at least 25 face recognition systems from 13 companies were available. Here is given different categories of Face recognition applications:

<table>
<thead>
<tr>
<th>Category</th>
<th>Exemplar application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face ID</td>
<td>Driver licenses, entitlement programs, immigration, national ID, passports, voter registration, welfare registration</td>
</tr>
<tr>
<td>Access control</td>
<td>Border-crossing control, facility access, vehicle access, smart kiosk and ATM, computer access, computer program access, computer network access, online program access, online transactions access, long distance learning access, online examinations access, online database access</td>
</tr>
</tbody>
</table>
Security
- Border-crossing control, facility access, vehicle access, smart kiosk and ATM, computer access, computer program access, computer network access, online program access, online transactions access, long distance learning access, online examinations access, online database access

Surveillance
- Advanced video surveillance, nuclear plant surveillance, park surveillance, neighborhood watch, power grid surveillance, CCTV control, portal control

Smart cards
- Stored value security, user authentication

Law enforcement
- Crime stopping and suspect alert, shoplifter recognition, suspect tracking and investigation, suspect background check, identifying cheats and casino undesirables, post-event analysis, welfare fraud, criminal face retrieval and recognition

Face databases
- Face indexing and retrieval, automatic face labeling, face classification

Multimedia management
- Face-based search, face-based video segmentation and summarization, event detection

Human computer interaction (HCI)
- Interactive gaming, proactive computing

Others
- Antique photo verification, very low bit-rate image & video transmission, etc.

| Table 2.2 – Application domains of Face recognition [5] |

The latest trends in face recognition include the self boarding with use of face recognition. Heathrow Airport passengers are among the first in the world to use biometric technology as part of a self-boarding gate solution. Terminal 1 passengers are being invited to take part in a two month ‘self-boarding’ trial in partnership with South African Airways. The trial is using facial biometric data to help them board their flight faster and more efficiently. Feedback from this trial has been positive, showing passengers are quick to adopt new technology to help streamline their journey through the airport [7].

This result tallies well against a recent survey by IATA. The Global Passenger Survey was formed as a result of nearly 3000 respondents from over 110 countries. It showed that of those respondents, 77% were comfortable using biometrics if available and 71% preferred to use self-boarding gates.

Current applications at Airports include the following:
1. Automated border control gates at immigration
2. Trusted traveler systems
3. Departure and boarding gates
4. Surveillance – Real time watch list alerts and Forensic video analysis
5. Queue management and flow analysis

2.2.6 Factors affecting success rate of face recognition

Here is the list of factors affecting the success rate of face recognition:

- Change in facial hair
- Change in hairstyle
- Lighting conditions
- Adding/removing hat
- Adding/removing glasses
- Change in weight
- Change in facial aspect (angle at which facial image is captured)
- Too much or too little movement
- Quality of capture device
- Change between enrollment and verification cameras (quality and placement)
- ‘Loud’ clothing that can distract face location

References