Biometrics.
What and how.

by

Moustafa Kamal El-Hadidi
k.moustafa@gmail.com
MIS Student,
Delta Academy for Science

Contents

1. **Introduction.**
2. **Biometric Systems.**
3. **Biometric System Errors.**
   - **3.1 False Acceptance Rate (FAR)**
   - **3.2 False Rejection Rate (FRR)**
4. **Biometric Technologies.**
   - **4.1 Biometric Process Flow.**
   - **4.2 Face**
   - **4.3 Iris**
   - **4.4 Ear**
   - **4.5 Voice**
   - **4.6 Fingerprint**
   - **4.7 Hand Geometry**
   - **4.8 Palmprint**
   - **4.9 Signature**
   - **4.10 Keystroke dynamics**
   - **4.11 Gait**
   - **4.12 Odor**
   - **4.13 Comparison of Biometric Technologies**
5. **Biometric Security Concerns.**
   - **5.1 Performance limitations.**
   - **5.2 Enrolment integrity.**
   - **5.3 Enrolment quality.**
   - **5.4 Spoofing (physiological biometrics).**
   - **5.5 Mimicry (behavioral biometrics).**
   - **5.6 Latent/Residual images.**
   - **5.7 Template integrity/confidentiality.**
   - **5.8 Capture/replay attacks.**
   - **5.9 Biometrics do not provide absolute identification.**
   - **5.10 Biometrics are not secret.**
   - **5.11 Biometrics are not random enough.**
   - **5.12 Biometric algorithms are proprietary and not validated.**
   - **5.13 Biometrics cannot be changed when compromised.**
   - **5.14 Biometrics do not offer non-repudiation.**
   - **5.15 How do we know when the system is becoming less secure?**
   - **5.16 Does publicizing countermeasures make the systems less secure?**
   - **5.17 Could I accidentally give my biometric 'signature'?**
   - **5.18 Can my biometric be collected covertly?**
   - **5.19 Can my biometric be stolen?**
6. **References.**

1. Introduction:

Humans have used body characteristics such as face, voice, gait, etc. from the day that mankind existed to recognize each other. Some characteristics don't change over time and some do. And since each on has a unique characteristics that no other share we humans have thought of using that in our daily life, The main aim of using it after 9/11 is for security reasons. So what characteristics do we use? Are they accurate?
Can we depend on them in our daily life routine?

I have tried to cover all of the characteristics that are used in Biometrics, How they are used, and what are the disadvantages of using them. So I hope that you find this document useful…

2. Biometric Systems:

A Biometric System is a pattern recognition system; it operates by acquiring biometric data from a person, extracting a feature set from the acquired data and comparing this feature against the templates in the database.

Biometric Technology can be divided into 2 major categories according to what they measure:
- Devices based on physiological characteristics of a person. (Fingerprint)
- Systems based on behavioral characteristics of a person. (Signature Dynamics)

Also biometric systems operate in 2 modes:
- Verification mode.
- Identification mode.

In verification mode, the system validates a person(s) identity by capturing biometric data and comparing it with his /her biometric template stored in the database.

In identification mode, the system recognizes a person by searching in all the templates in the database searching for a match.

3.1 False Acceptance Rate:
This is also known as type 2 error, False Acceptance Rate (FAR) is when an imposter is accepted as a legitimate user, This happens when the system find that the biometric data is similar to the template of a legitimate user.

3.2 False Rejection Rate:
False Rejection Rate (FRR) known as type 1 error, Is when a legitimate user is rejected because the system dose not find that the current biometric data of the user similar to the biometric data in the templates that are stored in the database.

Now since there is no zero error in a system that is in the real world, we calculate the FAR and the FRR using a simple math equation:

$$FAR(\lambda) = \frac{\text{Number of False Attempts}}{\text{Number of Impostor accesses}}$$

$$FRR(\lambda) = \frac{\text{Number of False Rejects}}{\text{Number of Client accesses}}$$

$$(\lambda) = \text{Security Level}$$

Now if we have a score of the FAR & FRR we can create a graph that indicates the depends of the FAR & FRR on the threshold value. The following (figure 1) is graph is an example:

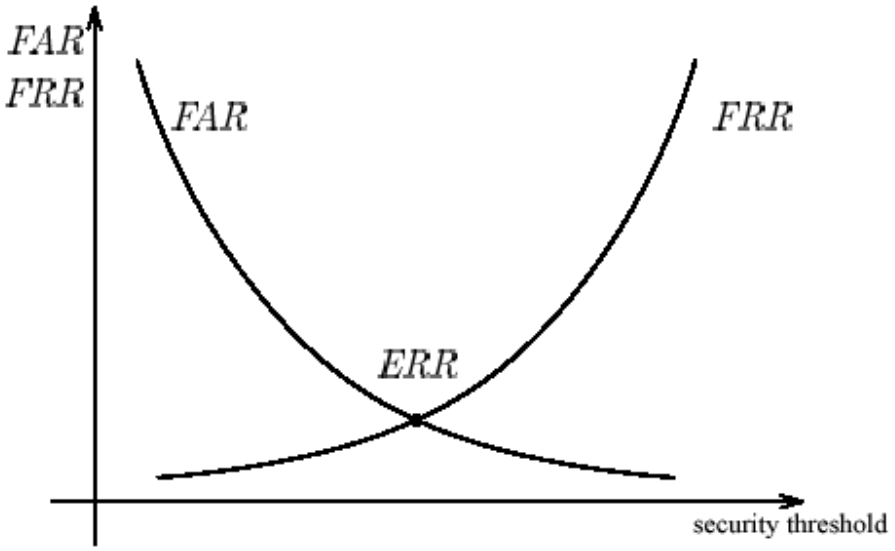


Figure 1

As we can see the curves of FAR and FRR cross at a point where FAR and FRR are equal, This value is called Equal Error Rate (ERR) or the Crossover Accuracy. The ERR is an indicator on how accurate the device is, the lower the ERR is the better the system.

If we have two devices with the equal error rates of 1% and 15% than we know that the first device with the ERR of 1% is more accurate than the other. Most manufactures often publish the best achieved rates (e.g. FAR < 0.01% and FRR < 0.1%) and not all manufactures use the same algorithms for calculating the rates.

4. Biometric Technologies:

4.1 Biometric Process Flow.

There is a step where the device acquires the biometric data and stores it into the template. This step is called: Enrollment, it consist of the following steps,
1- Data acquiring.
2. Creation of master characteristics.
3. Storage of master characteristics.

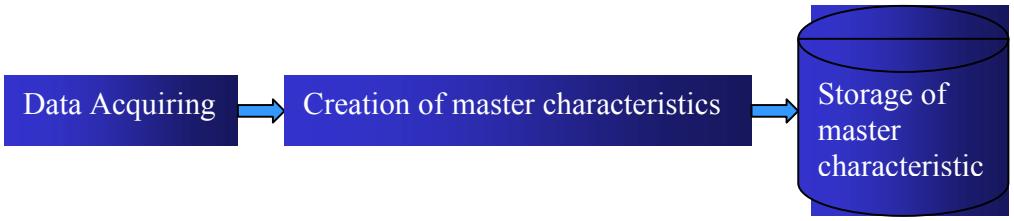


Figure 2 – Enrollment Steps.

1- Data Acquiring: In this step the user's biometric sample is obtained using an input device. The first biometric sample is the most important sample there is, thus it must be in good quality.

2- Creation of master characteristics: The biometric measurements are processed after the acquisition; the raw measurement contains a lot of irrelevant information. So the measurements are processed and only the important features are extracted and used.

3- Storage of master characteristics: After we have acquired the measurements we need to store them, there are four options possibilities on where to store them; each option depends on the use of the biometric data (e.g. ATM machine, Passport...Etc) and they are:

A- In a Card.
B- Central database on a server.
C- On a workstation.
D- In an authentication terminal.

The authentication or identification is similar to the enrollment process, with some differences. It consist of the following steps:

1- Acquisition
2- Creation of new characteristics.
3- Comparison.
4- Decision.

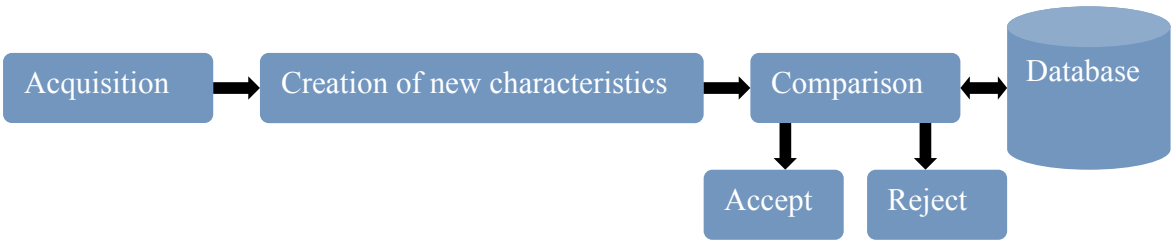


Figure 3 – Authentication Steps

1- Acquisition: The current biometric measurements must be obtained for the system to be able to make a comparison with the template that is has stored in the database.

2- Creation of new characteristics: The biometric measurements obtained in the acquisition step is processed and new characteristics are created, the process feature extraction is the same as the enrollment.

3- Comparison: The current obtained characteristics are than compared with the characteristics during the enrollment.

4- Decision: This is the final step in the verification process is the Accept / Reject decision based on the threshold.

Now since authenticating a person using biometrics consist of comparing a newly acquired Template $\boldsymbol{T}$ with a stored template $\boldsymbol{Ts}$. Some similarity measure $\mathbf{s} = \boldsymbol{S_M}\,(\boldsymbol{T}, \boldsymbol{Ts})$, which we can call a score, determines how similar the templates are. Decision are made based on a threshold $\boldsymbol{Th}$. A match is decided if $\mathbf{s} > \boldsymbol{Th}$ and a mismatch is decided if $\mathbf{s} < \boldsymbol{Th}$

In a more simple equation we can describe the verification and the verification problem.

a) An input feature: $\mathbf{X_Q}$
b) A claimed identity: **I**
c) The biometric template corresponds to **I** : $\mathbf{X_I}$
d) The similarity between $\mathbf{X_Q}$ and $\mathbf{X_I}$: $\mathbf{S(X_Q, X_I)}$
e) The predefined threshold of similarity : **t**
f) True: $\mathbf{W_1}$; False: $\mathbf{W_2}$

$$(I, X_Q) \in \begin{cases} \omega 1, & \text{if } S(X_Q, X_I) \geq t \\ \omega 2, & \text{otherwise} \end{cases}$$

When the biometric system process the verification there are two types of errors that the system can make:

1- Mistaking biometric measures from two different persons to be from the same person (false match)

2- Mistaking two biometric measurements from the same person to be from two different persons (false non-match)

Hypothesis testing for the errors that the system can make.

a) $\mathbf{H_0}$: input $\mathbf{X_Q}$ dose not come from the same person as the template $\mathbf{X_I}$
b) $\mathbf{H_1}$: input $\mathbf{X_Q}$ comes from the same person as $\mathbf{X_I}$

-Decision:
a) $\mathbf{D_0}$: person is not who they clam to be.
b) $\mathbf{D_1}$: person is who they clam to be.

If $\mathbf{S(X_Q, X_I) \geq t}$, then decide $\mathbf{D_1}$, else decide $\mathbf{D_0}$

In a hypothesis testing formulation contains two types of errors :
Type I (a) : false match **(D_1 , when H_0)**
Type II (β) : false non-match **(D_0 , when H_1)**

Also not that False Match Rate **(FMR)** is the probability of type I error, and False Non-match Rate **(FNMR)** is the probability of type II error.

4.2 Face:

There are two predominate approaches to face recognition: geometric (feature based) and photometric (view based). In this document I will talk about:

a) Principal Components Analysis (PCA)
b) Linear Discriminant Analysis (LDA)
c) Elastic Bunch Graph Matching (EBGM)

a) Principal Components Analysis (PCA):
Principal Components Analysis (PCA) is also known as **eigenfaces**.
Eigenfaces are a set of "standardized face ingredients" derived from statistical analysis of many pictures of faces. To generate a set of eigenfaces, a large set of digitized images of human faces taken under the same lighting conditions are normalized to line up the eyes and the mouth. They are than all resampled at the same pixel resolution (mxn) and than treated as mn-dimensional vectors who's components are the values of their pixels. The eigenvectors of the covariance matrix of the statistical distribution of face image vectors are then extracted. That was the definition of eigenfaces, We will see now the steps of that process.

Step 1 : obtain face images. $I_1, I_2, I_3, \ldots, I_M$
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 main face :

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

Step 5 : compute the covariance matrix **C** :

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

$$\text{where } A = [\Phi_1\ \Phi_2 \cdots \Phi_M] \quad (N^2 \text{x} M \text{ matrix})$$

Step 6 : compute the eigenvectors $\boldsymbol{u_i}$ of $\mathbf{AA^T}$
Step 6.1 : consider the matrix $\mathbf{A^T A}$ **(MxM matrix)**
Step 6.2 : compute the eigenvectors $\boldsymbol{v_i}$ of $\mathbf{A^T A}$

$$\mathbf{A^T A}\boldsymbol{v_i} = \boldsymbol{\mu_i}\, \boldsymbol{v_i}$$

The relationship between $\mathbf{us_i}$ and $\boldsymbol{v_i}$:

$$\mathbf{A^T A}\boldsymbol{v_i} = \boldsymbol{\mu_i}\, \boldsymbol{v_i} \Rightarrow \mathbf{AA^T A}\boldsymbol{v_i} = \boldsymbol{\mu_i}\, \mathbf{A}\boldsymbol{v_i} \Rightarrow \mathbf{CA}\boldsymbol{v_i} = \boldsymbol{\mu_i}\, \mathbf{A}\boldsymbol{v_i} \text{ Or } \mathbf{C}\boldsymbol{\mu_i} = \boldsymbol{\mu_i}\mathbf{u_i} \text{ where } \mathbf{u_i} = \mathbf{A}\boldsymbol{v_i}$$

And $\mathbf{AA^T}$ and $\mathbf{A^T A}$ have the same eignvalues and their eigenvectors are related as the following : $\mathbf{u_i} = \mathbf{A}\boldsymbol{v_i}$

Also note that :

1- $\mathbf{AA^T}$ can have up to $\mathbf{N^2}$ eigenvalues and eigenvectors.
2- $\mathbf{A^T A}$ can have up to **M** eigenvalues and eigenvectors.
3- The **M** eigenvalues of $\mathbf{A^T A}$ correspond to the **M** *largest* eigenvalues of $\mathbf{AA^T}$

Step 6.3 : compute the **M** best eigenvectors of $\mathbf{AA^T}$**:** $\mathbf{u_i} = \mathbf{A}\boldsymbol{v_i}$ also you must normalize $\mathbf{u_i}$ such that $\|\mathbf{u_i}\| = \mathbf{1}$

Step 7 : Keep only **K** eigenvectors, where **K** corresponds to the largest eigenvalues.

-Representing faces onto the basis, where each face $\boldsymbol{\Phi_i}$ in the training set can be represented as a linear combination of the best **K** eigenvectors :

$$\hat{\Phi}_i - mean = \sum_{j=1}^{K} w_j u_j, \quad (w_j = u_j^T \Phi_i)$$

we call the $\mathbf{u_j}$'s eigenfaces

-Each normalized training face $\boldsymbol{\Phi_i}$ is represented is this basis by a vector :

$$\Omega_i = \begin{bmatrix} w_1^i \\ w_2^i \\ \cdots \\ w_K^i \end{bmatrix}, \quad i = 1, 2, \ldots, M$$

-Face recognition using eigenfaces :

Given an unknown face image **Γ** follow these steps :

1- normalize **Γ: Φ = Γ – Ψ**
2- project on the eigenspace

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

3- represent **Φ** as:

$$\Omega = \begin{bmatrix} w_1 \\ w_2 \\ \dots \\ w_K \end{bmatrix}$$

4- find $\mathbf{e_r} = \mathbf{min_I} \|\mathbf{\Omega} - \mathbf{\Omega^I}\|$
5- if $\mathbf{e_r} < \mathbf{T_r}$ then **Γ** is recognized as face **I** from the training set.
The $\mathbf{e_r}$ is called distance within the face space (DIFS)

-Face detection using eigenfaces:

Given an unknown image **Γ** follow these steps :

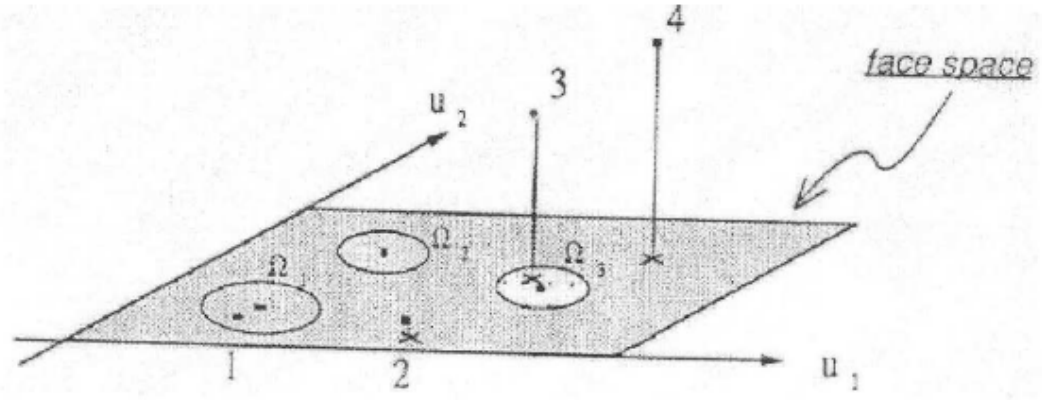
1- compute: $\mathbf{\Phi = \Gamma - \Psi}$
2- compute:

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

3- compute:

$$e_d = \|\Phi - \hat{\Phi}\|$$

4- if $\mathbf{e_d} < \mathbf{T_d}$ then **Γ** is a face.
The $\mathbf{e_d}$ is called distance from face space (DFFS)



b) Linear Discriminant Analysis (LDA):

Linear Discriminant Analysis (LDA) is a well-known scheme for feature extraction and dimension reduction. It has been used widely in many applications involving high-dimensional data, such as face recognition. The goal of LDA is to perform dimensionality reduction while preserving as much of the class discriminatory information as possible.

- The Math behind LDA :

1- Suppose there are **C** classes.
2- μ_i the main vector of class i, i = 1,2,3,..,**C**
3- $\mathbf{M_i}$ the number of samples within classes i, I = 1,2,3,..,**C**
4- The total number of samples :

$$M = \sum_{i=0}^{C} M_i$$

Within-class scatter matrix:

$$S_w = \sum_{i=1}^{C} \sum_{j=1}^{M_i} (y_j - \boldsymbol{\mu}_i)(y_j - \boldsymbol{\mu}_i)^T$$

Between-class scatter matrix:

$$S_b = \sum_{i=1}^{C} (\boldsymbol{\mu}_i - \boldsymbol{\mu})(\boldsymbol{\mu}_i - \boldsymbol{\mu})^T$$

$$\boldsymbol{\mu} = 1/C \sum_{i=1}^{C} \boldsymbol{\mu}_i \quad \text{(mean of entire data set)}$$

5- LDA computes a transformation that maximizes the between-class scatter while minimizing the within-class scatter :

$$\text{maximize } \frac{det(S_b)}{det(S_w)}$$

-Linear transformation implied by LDA :

1- The linear transformation is given by a matrix **U** whose columns are the eigenvectors of $S_w^{-1} S_b$ (called Fisherfaces)

$$\begin{bmatrix} b_1 \\ b_2 \\ \dots \\ b_K \end{bmatrix} = \begin{bmatrix} u_1^T \\ u_2^T \\ \dots \\ u_K^T \end{bmatrix} (x - \boldsymbol{\mu}) = U^T (x - \boldsymbol{\mu})$$

2- The eigenvectors are solutions of the generalized eigenvector problem:

$$S_B u_k = \lambda_k S_w u_k$$

3- There are at most **C** – 1 non-zero generalized eigenvectors.

c) Elastic Bunch Graph Matching (EBGM):

Elastic Bunch Graph Matching (EBGM) uses the structure information of a face which reflects the fact that the images of the same subject tend to translate, scale, rotate, and deform in the image plane. It makes use of the labeled graph, edges are labeled the distance information and nods are labeled with wavelet coefficients in jets. This model graph can then be used to generate image graph. The model graph can be translated, scaled , rotated and deformed during the matching process. Gabor.

-Processing using Gabor Wavelets :

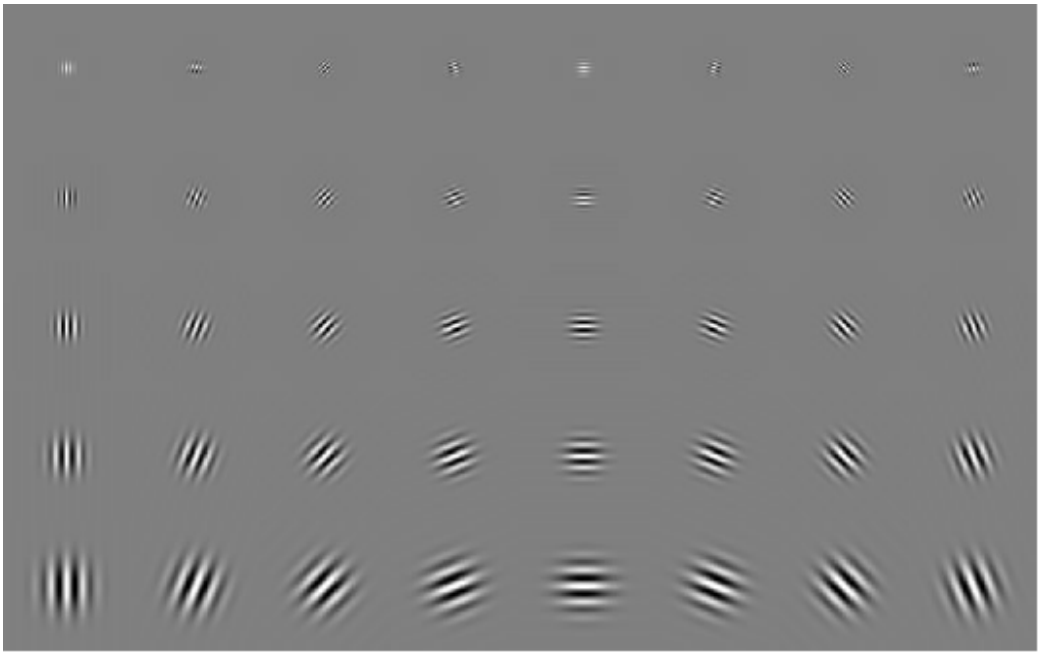


Figure 4 - The real part of the Gabor filter with 5 frequencies and 8 orientations

Gabor wavelet transformation is used to represent the local features of the face images. Gabor wavelets are biologically motivated convolution kernels in the shape of plan waves restricted by a Gaussian envelop function, the set of convolution coefficients for kernels of different orientations and frequencies at one image pixel is called a jet.

- Jet:
A jet means a set of gray values in an image $\mathbf{I(x^w)}$ around a given pixel $\mathbf{x^w = (x,y)}$, which is based on wavelets transformation, defined as a convulsion

$$J_j(\vec{x}) = \int I(\vec{x}')\psi_j(\vec{x} - \vec{x}')d^2\vec{x}'$$

With a family of Gabor kernels:

$$\psi_j(\vec{x}) = \frac{k_j^2}{\sigma^2}\exp\left(-\frac{k_j^2 x^2}{2\sigma^2}\right)\left[\exp\left(i\vec{k}_j\vec{x}\right) - \exp\left(-\frac{\sigma^2}{2}\right)\right]$$

in the shape of plan waves with wave vector $\mathbf{K}^{w}_{j}$, the function is restricted by a Gaussian envelope function:

$$\exp\left(-\frac{k_j^2 x^2}{2\sigma^2}\right)$$

Using 5 different frequencies, index **v= 0,…,4** and **8** orientations, index **μ=0,…,7,**

$$\vec{k}_j = \begin{pmatrix} k_{jx} \\ k_{jy} \end{pmatrix} = \begin{pmatrix} k_v \cos\varphi_u \\ k_v \sin\varphi_u \end{pmatrix}, k_v = 2^{-\frac{v+2}{2}}\pi, \varphi_u = \mu\frac{\pi}{8},$$

with index **j = μ + 8v** the width **σ / k** of the Gaussian is controlled by the parameter **σ = 2π.** The second term is the bracket of Eq. **(8)** makes the kernel DC-free. I.e.: the integral $\int \psi_j(\vec{x})d^2\vec{x}$ vanishes. All kernels are generated from one mother wavelet by dilation and rotation because the family of kernels is self-similar. A jet **j** is defined as the set **{j_i}** of 40 complex coefficients for one image point

$$\mathbf{j_i = a_j \exp(i\varnothing_j)}$$

where $\mathbf{a_j}$ is the magnitudes $a_j(\vec{x})$, which slowly vary with position, and phases $\phi_j(\vec{x})$, which rotate at a rate approximately determined by the spatial frequency or wave vector $\mathbf{K}^{w}_{j}$ of the kernels.

- Comparing Jets:

Jets taken from image points only a few pixel apart from each other have very different coefficient due to the characteristics of phase rotation, this can cause problems for matching. That is why we either ignore the phase compensate for it.

$$S_a(J,J') = \frac{\sum_j a_j a'_j}{\sqrt{\sum_j a_j^2 \sum_j a'^2_j}},$$

This is a smooth function with local optima forming the large attraction basins leading to rapid and reliable convergence with simple search method. Pattern between similar magnitude can be discriminated by using phase information, and the accurate jet localization in an image can also be found because phase varies so quickly with location.

Assuming that two jets **J** and **J'** refer to the locations with small relative displacement $\mathbf{d}^{\mathbf{w}}$ The phase shifts can be approximately compensated for by the term $\mathbf{d}^{\mathbf{w}}\mathbf{k}^{\mathbf{w}}_{\mathbf{j}}$ this form a phase-sensitive similarity function

$$S_\phi(J,J') = \frac{\sum_j a_j a'_j \cos\left(\phi_j - \phi'_j - \vec{dk}_j\right)}{\sqrt{\sum_j a_j^2 \sum_j a'^2_j}}.$$

To estimate the displacement $\mathbf{d}^{\mathbf{w}}$ we can maximize $\mathbf{S}_{\boldsymbol{\phi}}$ in its Taylor expansion, To find the displacement vector $\mathbf{d}^{\mathbf{w}} = (\mathbf{d}_x, \mathbf{d}_y)$ disparity estimation method is used. That is maximization of the similarity $\mathbf{S}_{\boldsymbol{\phi}}$ in its Taylor expansion

$$S_\phi(J,J') \approx \frac{\sum_j a_j a'_j \left[1 - 0.5\left(\phi_j - \phi'_j - \vec{dk}_j\right)^2\right]}{\sqrt{\sum_j a_j^2 \sum_j a'^2_j}}.$$

By setting $\frac{\partial}{\partial d_x} S_\phi = \frac{\partial}{\partial d_y} S_\phi = 0$ and solving for $\mathbf{d}^{\mathbf{w}}$ yield

$$\overline{\overline{\omega}}\overline{d}(J, J') = \begin{pmatrix} d_x \\ d_y \end{pmatrix} = \frac{1}{\Gamma_{xx}\Gamma_{yy} - \Gamma_{xy}\Gamma_{yx}} \times \begin{pmatrix} \Gamma_{yy} & -\Gamma_{yx} \\ -\Gamma_{xy} & \Gamma_{xx} \end{pmatrix} \begin{pmatrix} \Phi_x \\ \Phi_y \end{pmatrix},$$

if $\mathbf{\Gamma_{xx}\Gamma_{yy} - \Gamma_{xy}\Gamma_{yx} \neq 0}$, with

$$\Phi_x = \sum_j a_j a'_j k_{jx} (\phi_j - \phi'_j),$$

$$\Gamma_{xy} = \sum_j a_j a'_j k_{jx} k_{jy},$$

and $\mathbf{\Phi_y}$, $\mathbf{\Gamma_{xx}\Gamma_{yx}\Gamma_{yy}}$ defined correspondingly. In this function the phase differences may exist the range of $\pm \boldsymbol{\pi}$, we need to correct it by $\pm \mathbf{2\pi}$. The displacement can be estimated between two jets when they are close enough that their Gabor kernels are highly overlapping.

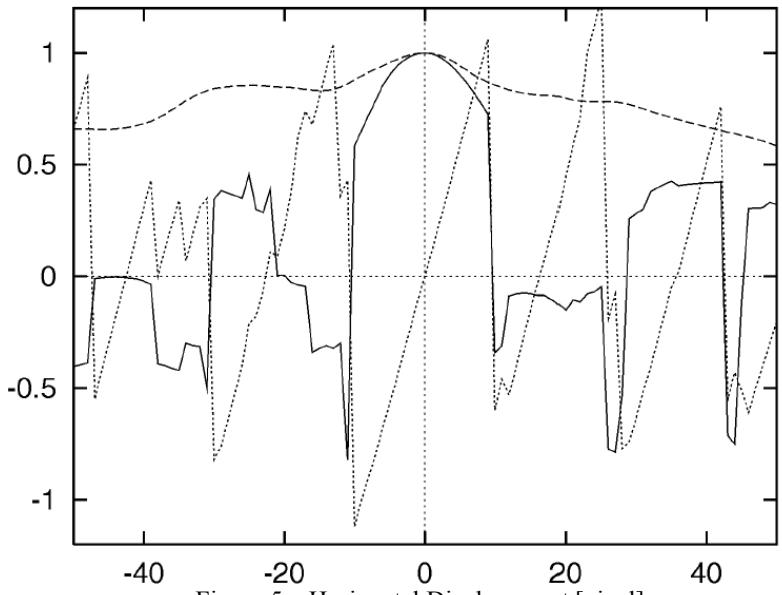


Figure 5 – Horizontal Displacement [pixel]
similarity without phase (a) **:** **-----**
similarity with phase (b) : _____
estimated displacement /8 (c) : ---------

Figure 5 (a) Similarity $S_a\left(J\left(\vec{x}_1\right), J'\left(\vec{x}_0\right)\right)$ with **J**' taken from the left eye of the face and **J** taken from the same horizontal line with jet

$$J', \quad \vec{x}_1 = \vec{x}_o + (d_x, 0), d_x = -50,...,50$$

(b) Similarity $S_\phi\left(J\left(\vec{x}_1\right), J'\left(\vec{x}_0\right)\right)$ and (c) estimated displacement $\vec{d}\left(J\left(\vec{x}_1\right), J'\left(\vec{x}_0\right)\right)$ for the same jet (a) using focus 1.

The similarity function without phase is smooth function which in a range of 0.6-1.0, and we can roughly find there is a local maximum around $\mathbf{d}^{\mathbf{w}}_{\mathbf{x}} = \mathbf{-24}$ as the right eye is 24 pixel away from the left eye, we cant locate the jet precisely so we use the similarity function with phase. The estimated displacement is periodic due to the frequency of the kernel. Without modifications the equation $\mathbf{S_\theta}$ can determine displacement up to half the wavelength of the highest frequency kernel, which would be two pixel for $\mathbf{k_0 = \pi/2}$ The estimated range can be increased by using low frequency kernels only. We refer to the number of frequency levels used for the first displacement estimation as focus. A focus 1 means that only the lowest frequency level is used and the estimated range may be up to 8 pixels. For each higher level the phases of the higher frequency coefficients have to be corrected by multiples of $\mathbf{2\pi}$ to match as closely as possible to the expected phase differences inferred from the displacement estimated on the lower frequency level.

-Face Representation:

A) Individual Faces:

To represent a face we use a set of fiducial points (the pupil, eyebrows,..etc) A labeled graph **G** representing the face consists of **N** nodes on these fiducial points at position $\vec{x}_n, n = 1,..., N$ and **E** edges between them. Each node are labeled with jets $\mathbf{J_n}$. The edges are labeled with distances $\Delta\vec{x}_e = \vec{x}_n - \vec{x}_{n'}, e = 1,..., E$ where edge **e** connects node **n** with **n**' . This face graph is object-adapted, since most nodes are selected from face-specification point. The position of the jet is selected manually as some of the nodes maybe occluded and the distance vary due to rotation in depth.

B) Face Bunch Graph:

Automatic finding fiducial points in new faces need a general representation rather than models of the individual faces. A wide range of possible variations in the appearance of faces, like different shaped eyes, mouth, variation due to sex, age, etc, should be covered.

Combination each feature by a separate graph is not efficient. So we use a stack like structure called a face bunch graph **(FBG)**

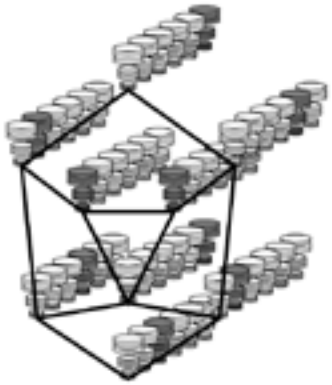


Figure 6 – The face Bunch Graph represent the face in general.

Each model has the same grid and structure and the nodes refer to the identical fiducial points. A set of jets referring to one fiducial point is called a bunch. During the location of each fiducial point in a face, the best fitting jet called the local expert is selected from the bunch. So any combination of jets in the bunch graph is available for a wide range of variation than the model of individual faces. To form a **FBG**, assume for a practical pose that there are **M** model graphs $\mathbf{G^{Bm}}$ **(m=1,…,M)** of identical structure, taken from different model faces. The corresponding **FBG B** is then given the same structure, its nodes are labeled with bunches of jets $\mathbf{J^{Bm}_n}$ and its edges are labeled with the averaged distance

$$\Delta\vec{x}_e^{B} = \sum_m \Delta\vec{x}_e^{Bm} / M .$$

Increasing the number of variant of **FBG** also increases with the desired matching accuracy for finding the fiducial points in a new face. But in general the models in the **FBG** should be as different as possible to reduce redundancy and maximize variability.

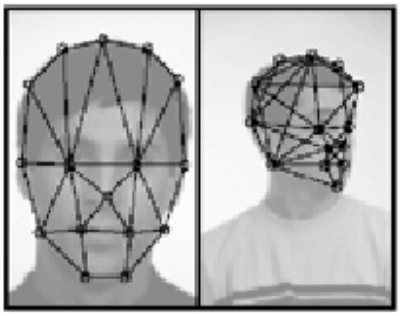
C) Generating Face Representation by Elastic Bunch Graph Matching:

After description for the individual faces and **FBG**, we will talk about how these graphs are generated. One of the simplest method is to select fiducial points manually, This is used for the generation of initial graphs for the system. **FBG** can then be formed, new images can be generated automatically by Elastic Bunch Graph Matching.

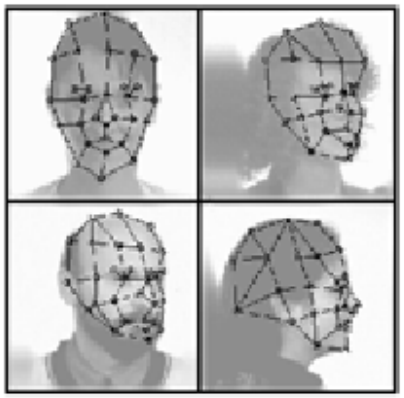
C.1) Manual Definition of Graphs:

Manual definition of graphs involves three steps :

1- Mark a set of fiducial points of a given image.
2- The edges are drown between fiducial points and edge labels are automatically computed as the differences between node postions.
3- Use Gabor wavelet transform to compute the jet for the nods.



Grids for face finding



Grids for face recognition

C.2) The Graph Similarity Function:

The graph similarity an image graph and the **FBG** of identical pose play a key role in Elastic Bunch Graph Matching. It depends on the jet similarity and the distortion of the image grid relative to the **FBG** grid. The similarity function is :

$$S_B\left(G^I, B\right) = \frac{1}{N}\sum_n \max_m\left(S_\phi\left(J_n^I, J_n^{Bm}\right)\right) - \frac{\lambda}{E}\sum_e \frac{\left(\Delta\vec{x}_e^{\,I} - \Delta\vec{x}_e^{\,B}\right)^2}{\left(\Delta\vec{x}_e^{\,B}\right)^2}$$

Where $\mathbf{G^1}$ is an image graph with node **n =1,…,N** and edges **e = 1,…,E** , **FBG B** with model graph **m = 1,…,M** and **λ** determine the relative importance of jets and metric structure. $\mathbf{J^n}$ are the jets at node **n** and $\Delta\vec{x}_e$ are the distance vectors used as labels at edges **e.** The first term is feature (Jet) comparison term and the second term is metric comparison term (Distortions).

4.3 Iris / Retinal scan:

Iris recognition is the process of recognizing by analyzing the random pattern of the iris. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle.

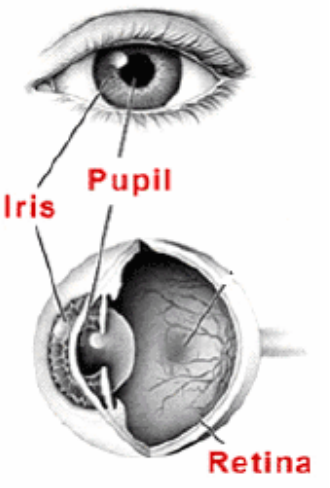


Figure 1: Iris Diagram

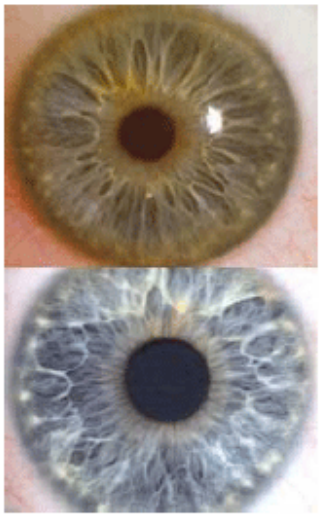


Figure 2: Iris Structure.

Although the coloration and structure of the iris is genetically linked, the details of the patters are not. The iris develops during prenatal growth through a process of tight forming and folding of the tissue membrane. Before recognition of the iris takes place, the iris is located using landmark features. These landmark features and the distinct shape of the iris allow for imagining, feature isolation, and extraction. Localization of the iris is an important step in iris recognition, if done improperly, resultant noise in the image may lead to poor performance.

To capture the details of the iris patterns an imaging system should resolve a minimum of 70 pixels in iris radius. Images passing a minimum focus criterion are then analyzed to find the iris, with precise localization of its boundaries using a coarse-to-fine strategy terminating in single-pixel precision estimated of the center of coordinates and radius of both the iris and the pupil. Although the result of the iris search greatly constrain the pupil search concentricity of these boundaries cannot be assumed, very often the pupil center is nasal and inferior to the iris center. Its radius can range from 0.1 to 0.8 of the iris radius, thus all three parameters defining the pupillary circle must be estimated separately from those of the iris. A very effective integrodifferential operate for determining these parameters is:

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} \, \mathrm{d}s \right|$$

Where **I(x,y)** is an image containing an eye, the operator searches over the image domain **(x,y)** for the maximum in the blurred partial derivative with respect to increasing radius **r** of the normalized contour of integral of **I(x,y)** along a circle arc **ds** of radius **r** and centre coordinates **(x_0,y_0).** The symbol ***** denotes convolution and **G_σ(r)** is a smoothing function such as **Gaussian** of scale **σ**. The complete operator behaves in effect as a circular edge detector blurred at a scale set by **σ**, which searches iteratively for a maximum contour integral derivative with increasing radius at successively finer scales of analysis through the three parameter space of center coordinates and radius **(x_0,y_0,r)** defining a path of contour integration. The operator in the past equation serves to find both the pupillary boundary and the outer (limbus) boundary of the iris. Although the initial search for the limbus should incorporate evidence of an interior pupil to improve its robustness since the limbic boundary itself usually has extremely soft contrast when long-wavelength **NIR** illumination is used.Once the coarse-to-find iterative searches for both these boundaries have reached single pixel precision, then a similar approach to detecting curvilinear edges is used to localize both the upper and lower eyelid boundaries. The path of contour integration in the past equation is changed from circular to arcuate with spline parameters fitted by standard statistical estimation methods used to describe optimally the available evidence for each eyelid boundary. The result of all these localization operations is the isolation of iris tissue from all other image regions, as illustrated in Figure 3 by the graphical overlays on these two eyes.

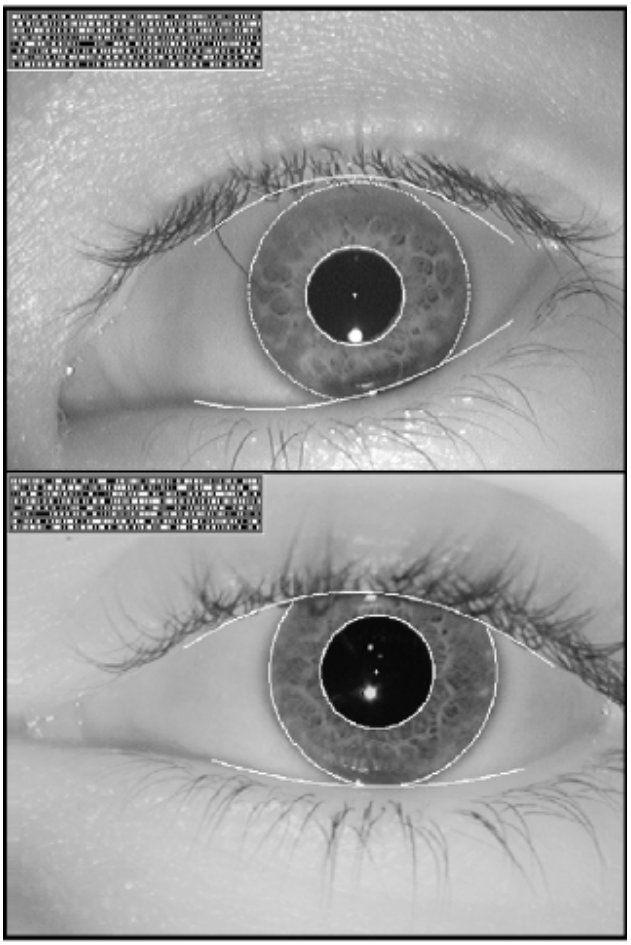


Figure 3

A.1) Iris feature encoding by 2D wavelet demodulation:

Each isolated iris pattern is then demodulated to extract its phase information using quadrature 2D **Gabor** wavelets. This encoding process is illustrated in Figure 4. It amounts to a patch-wise phase quantization of the iris pattern, by identifying in which quadrant of the complex plane each resultant phasor lies when a given area of the iris is projected onto complex-valued 2D.

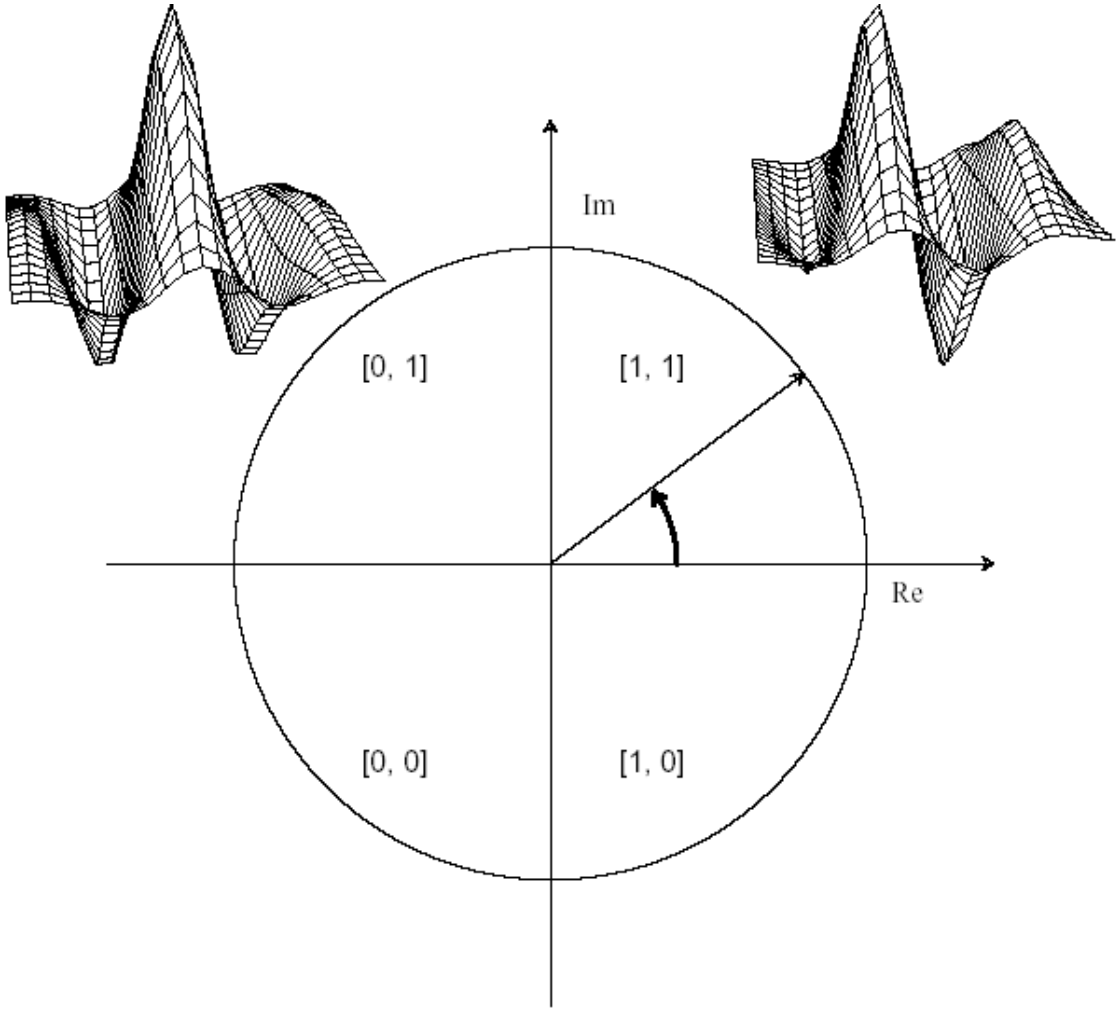


Figure 4

Gabor wavelets:

$$h_{\{Re,Im\}} = \mathrm{sgn}_{\{Re,Im\}} \int_{\rho}\int_{\phi} I(\rho,\phi)\mathrm{e}^{-\mathrm{i}\omega(\theta_0-\phi)}\mathrm{e}^{-(r_0-\rho)^2/\alpha^2}$$

$$\times \mathrm{e}^{-(\theta_0-\phi)^2/\beta^2}\,\rho\,\mathrm{d}\rho\,\mathrm{d}\phi,$$

Where $h_{\{Re,Im\}}$ can be regarded as a complex-valued bit whose real and imaginary parts are either 1 or 0 (sgn) depending on the sign of the 2D integral; $I(\rho,\phi)$ is the raw iris image in a dimensionless polar coordinate system that is size- and translation-invariant, and which also corrects for pupil dilation as explained in a later section; α and **β** are the multi-scale 2D wavelet size parameters, spanning an 8-fold range from 0.15 to

1:2 mm on the iris; **ω** is wavelet frequency, and **(r_0,θ_0)** represent the polar coordinates of each region of iris for which the phasor coordinates $h_{\{Re,Im\}}$ are computed. Such a phase quadrant coding sequence is illustrated for two irises by the bit streams pictured in Figure 3. Desirable feature of the phase code explained in Figure 4 is that it is a cyclic or Gray code: in rotating between any adjacent phase quadrants, only a single bit changes, unlike a binary code in which two bits may change, making some errors arbitrarily more costly than others. Altogether 2048 such phase bits (256 bytes) are computed for each iris, but in a major improvement over the earlier Daugman algorithms, now an equal number of masking bits are also computed to signify whether any iris region is obscured by eyelids, contains any eyelash occlusions, specular reflections, boundary artifacts of hard contact lenses, or poor signal-to-noise ratio and thus should be ignored in the demodulation code as artifact. Only phase information is used for recognizing irises because amplitude information is not very discriminating, and it depends upon extraneous factors such as imaging contrast, illumination, and camera gain. The phase bit settings which code the sequence of projection quadrants as shown in figure 4 capture the information of wavelet zero-crossings, as is clear from the sign operator in the past equation. The extraction of phase has the further advantage that phase angles are assigned regardless of how poor the image contrast may be, as illustrated by the extremely out-of-focus image in figure 5. Its phase bit stream has statistical properties such as run lengths similar to those of the code for the properly focused eye images in figure 3 the benefit which arises from the fact that phase bits are set also for a poorly focused image as shown here, even if based only on random CCD noise, is that different poorly focused irises never become confused with each other when their phase codes are compared. By contrast, images of different faces look increasingly alike when poorly resolved, and may be confused with each other by face recognition algorithms.

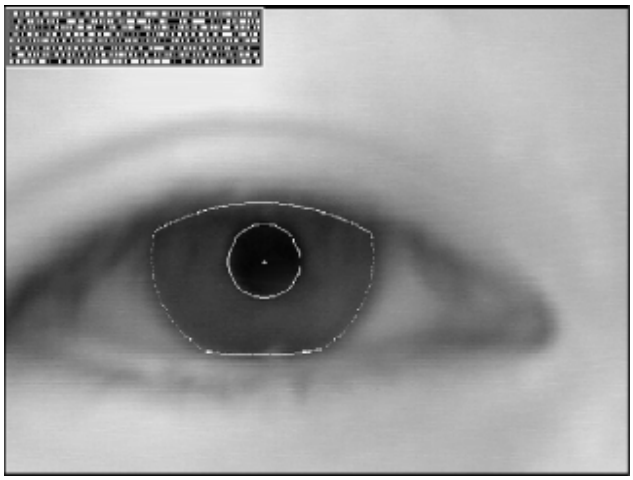


Figure 5

4.4 Ear:

There are many approaches for ear identifications, but here i will talk about the ear identification made by Alfred Iannarelli.

There are three methods for ear identification :
1- taking a photo of the ear.
2- taking earmarks by pushing the ear against a flat glass.
3- taking thermogram picture of the ear.

Alfred Iannarelli defined a system that is called “Iannarelli System” which is a anthropometric technique based upon the 12 ear measurements, it requires exact alignment and normalization of the ear photo allows comparable. The distance between each of the numbered areas in the measured in units of 3mm and assigned an integer distance value. The identification consists of 12 measurements and the information about sex and race.

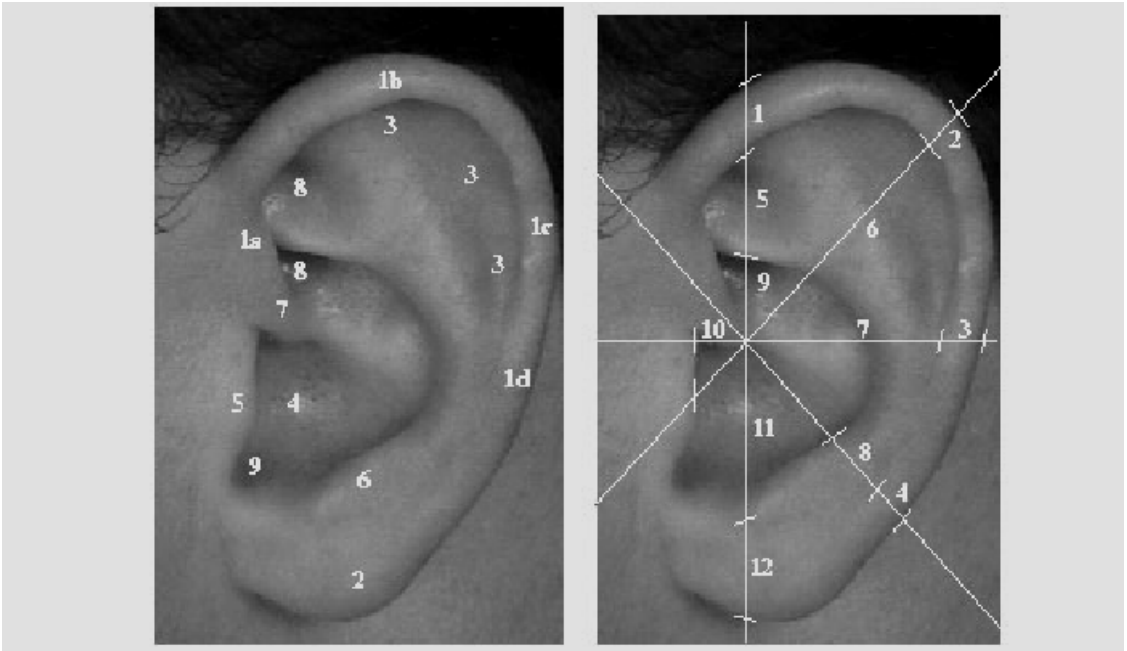


Figure 6 (a) Anatomy, (b) Measurements. (a) 1 Helix Rim, 2 Lobule, 3 Antihelix, 4 Concha, 5 Tragus, 6 Antitragus, 7 Crus of Helix, 8 Triangular Fossa, 9 Incisure Intertragica. (b) The locations of the anthropometric measurements used in the “Iannarelli System”.

Earmarks: is where the ear is pressed against some materials such as glass and earmark can be used as biometric. However the earmark usually doses not have enough details for reliable identification.

Thermogram Pictures: In the thermogram pictures different colors and textures are used to find the different parts of the hair and isolate it from the ear itself. In figure 7 the hair is between 27.2 and 29.7 degrees Celsius while the outer ear areas range from 30.0 to 37.2 degrees Celsius, the ear is easy to locate and localizable using thermogram images by searching for high temperature areas.

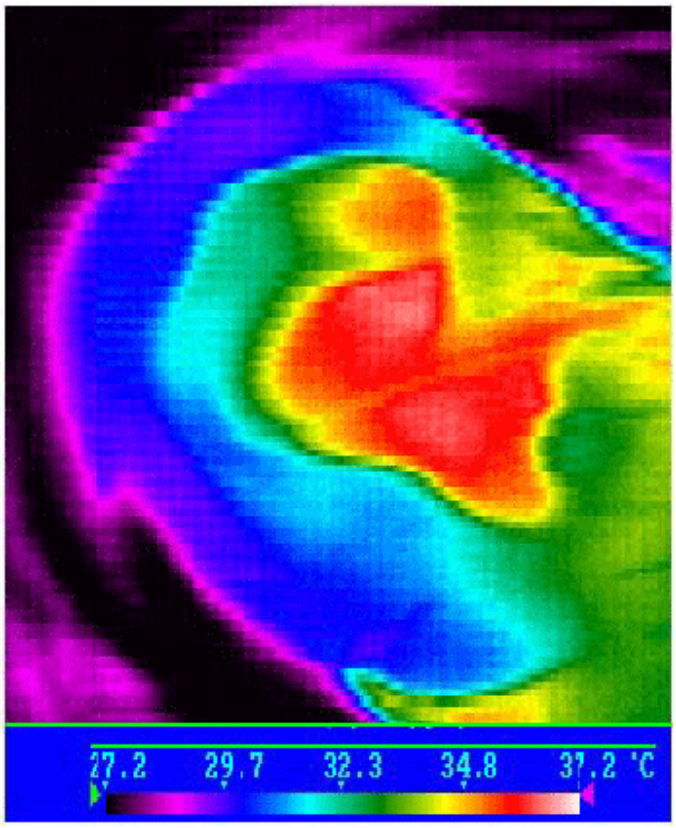


Figure 7 Thermogram of an ear. Image provided by Brent Griffith, Infrared Thermography Laboratory, Lawrence Berkeley, National Laboratory.

4.5 Voice:

Voice verification focus on the vocal characteristics that produce speech and not on the sound or the pronunciation of the speech itself, the vocal characteristics depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanisms of the human body.

There are two forms of speech recognition:

1- text depended.
2- text independent.

In text depended speech, the person presents either a “fixed password” or promoted to say a certain phrase that is programmed in the system such as (please say : 52-hi-95). In text independent speech, the system has no advance knowledge of the phrase, during the enrollment or collection phase, the person says a short word a phrase (utterance), The voice sample is converted from analog format to digital format, the features on the persons voice are extracted and than a model is created.

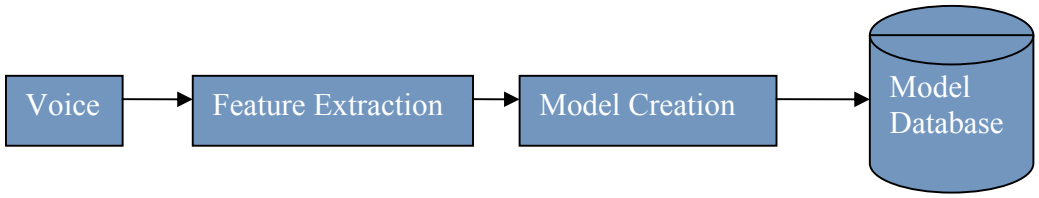


Figure 8 the enrollment process

Most text dependent systems use the concept of **Hidden Markov Models (HMMs)** where random based models that provide a statistical representation of the sounds produced by the person. The **HMM** represents the underlying variations and temporal changes over the time found in the speech states using the quality – duration – intensity dynamics – pitch characteristics. Another method is the **Gaussian Mixture Model.** A state-mapping model closely related to **HMM.** This method uses the voice to create a number of vector “states” representing the various sound forms, which are characteristic of the physiology and behavior of the person.

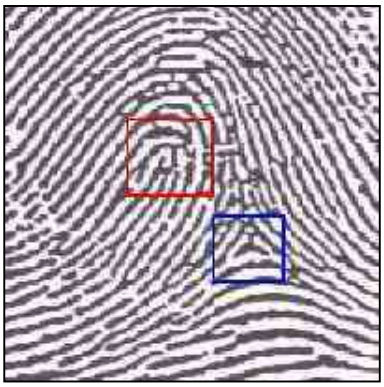
Text-Dependent Recognition	Text-Independent Recognition
-Recognition system knows text spoken by a person. -Fixed Phrases, Prompted Phrases. -Used for applications with strong control over user input. -Knowledge of spoken text can improve system performance.	-Recognition system dose not know the text spoken by a person. -User selected phrases. -Used for applications with less control over user input. -More flexible system but also more difficult problem.

Figure 9 Speech Modality

4.6 Fingerprint:

A fingerprint is an impression of the friction ridges of all or any part of the finger.A friction ridge is a raised portion of the epidermis on the palmar (palm and fingers) or plantar (sole and toes) skin, consisting of one or more connected ridge units of friction ridge skin. These ridges are sometimes known as "dermal ridges" or "dermal papillae". In the Henry system of classification, there are three basic fingerprint patterns: Arch, Loop and Whorl. There are also more complex classification systems that further break down patterns to plain arches or tented arches. Loops may be radial or ulnar, depending on the side of the hand the tail points towards. Whorls also have sub-group classifications including plain whorls, accidental whorls, double loop whorls, and central pocket loop whorls. So lets have a look at the different patterns :

-Loops:
Loops constitute between 60 and 70 per cent of the patterns encountered. In a loop pattern, one or more of the ridges enters on either side of the impression, recurves, touches or crosses the line of the glass running from the delta to the core, and terminates or tends to terminate on or in the direction of the side where the ridge or ridges entered. There is one delta. On the right you will see a loop pattern. You will notice that it has one delta (shown in the blue box) and a core (shown in the red box). By definition the existence of a core and one delta makes this pattern a loop.



Loops are classified not only by the fact that they have one delta and one core but also by something called a ridge count. Loops are two kinds, 'radial' and 'ulnar', named after the radius and ulna, the two bones in the forearm. The radius joins the hand on the same side as the thumb, and the ulna on the same side as the little finger.

-Radial Loops:

The distinction between Ulnar and Radial loops depends on which hand the loop is found on. In the image at left the core pattern area (noted in red) tends to come in from the left and go back out the left. Hold your left hand up to the screen and note that your little finger is on the left, which is the direction that the pattern tends to come in from and go back out to. Since this is towards your little finger, and by virtue of that towards your ulnar bone in your arm, this makes the loop an ulnar loop. Now, if you were to place your

right hand up to the screen and make the same comparison you would find that the pattern area now tends to come in and go out towards your thumb. It so happens that the radial bone in your arm is on your thumb side so now this loop would be considered a radial loop. Obviously to make the distinction between these two types of loops you have to know on which hand they appear because if a loop pattern is an Ulnar loop on the right hand, then by default it will be a Radial loop if found on the left hand.
Radial loops are not very common. Most of the time if you find a radial loop on a person it will usually be on the index fingers.

-Whorls:

Between 25 and 35 per cent of the patterns encountered consist of whorls. In a whorl, some of the ridges make a turn through at least one circuit. Any fingerprint pattern which contains 2 or more delta's will be a whorl pattern. In the scheme of classification you can make the assumption that if a pattern contains no delta's then it is an arch, if it contains one (and only one) delta it will be a loop and if it contains 2 or more it will always be a whorl. If a pattern does contain more than 2 delta's it will always be an accidental whorl.


Plain


Central Pocket


Double Pocket


Accidental

-Plain Whorls:

As with any whorl there must be more than 1 valid delta or else it is a loop. If you look at image a you should be able to identify the two delta's. If not then look at image B and you will see that they are displayed in the red boxes. The technical definition of a plain whorl is a whorl which consists of one or more ridges which make or tend to make a complete circuit, with two delta's, between which an imaginary line is drawn and at least one recurving ridge within the inner pattern area is cut or touched.

Notice the inner area of the pattern that is the area which tends to form a circle? This is what you would call the inner pattern area and it is what make a whorl look like a whorl. Okay, now looking at the specific ridges that are making or trying to make the circle lets say we were to draw an imaginary line between the two delta's (the red line in image C)

then we can see that this line does intersect the same lines or line that tend to form the circle.

A **B** **C**

Alright now let's take a closer look so maybe this will become more clear about what is sufficient and what is not sufficient to be a plain whorl.

D **E** **F**

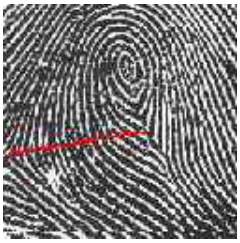
Take a look at image D and you can see the inner pattern area in yellow that forms or tends to form the circle part of the loop. Notice now that if we draw a line from delta-to-delta we do not intersect the lines that are forming the circle? The same thing is true for image E. Take a look at image E and see if you can determine the inner pattern, that being the ridges that form or tend to form a circle. Can you see that if a line is drawn again from delta-to-delta that no lines that form the circle are intersected? Now look at image F and see if you can identify the ridges that are forming or tending to form the circle or inner pattern. Notice now that when we draw a line from delta-to-delta that this inner pattern or the lines forming the circle are intersected? Image D and image E are examples of Central Pocket whorls. Image F is a plain whorl. This is the first part of identifying a particular whorl. In this process we merely identified the pattern type. In this case we have identified what it takes to be a plain whorl.

-Central Pocket Whorls:

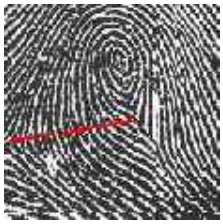
A central pocket whorl consists of at least one recurving ridge, or an obstruction at right angles to the line of flow, with two deltas, between which when an imaginary line is drawn, no recurving ridge within the pattern area is cut or touched.


G


H


I

If you look at the pattern area of the three images at left you will notice that the actual lines that make a "circle" are very close to the centre and there are not very many of them, in fact only about two or three on Image G and about the same on image H. To make the determination of the type of pattern we must draw an imaginary line between the two deltas that appear on the print. In image i have drawn a red line to act as the imaginary line between the two deltas and if you study this you will see that the ridges that form the inner pattern are not crossed by this imaginary line. This makes it a central pocket whorl by definition. If the ridges of the inner pattern were crossed then this would be a plain whorl. Let's looks at some comparisons between a central pocket whorl and the other types: When compared side-by-side the differences become a little more obvious. If you look at image G you can see that the imaginary line (in red) does not cut across any ridges which form the inner pattern area. But if you look at image H you can see that the imaginary line does, in fact, cut across the inner pattern area (or the ridges which form or tend to form a circle). The pattern in image I might at first glance be taken for a plain whorl because if you were to draw the imaginary line it would cut the pattern area, but you will notice there are two core area's in this pattern, which are shown by the red pointers. Because of the two cores this pattern is a double loop whorl.


Central Pocket


Plain Whorl

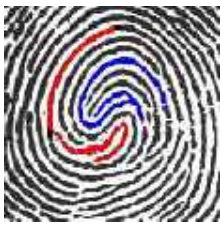

Double Whorl

-Double Loop Whorls:

A double loop whorl consists of two separate and distinct loop formations with two separate and distinct shoulders and two deltas. The technical definition for this pattern type is fairly straight-forward. There must be to separate and distinct shoulders for each core. If you look at images J and image K you can clearly see that there appears to be two separate "loops" inside of this whorl. In most cases this means that the pattern will most likely be a double loop whorl but not always. The problems lie in the "separate and distinct" shoulder requirement sometimes. If you look at image L you can clearly see that there are separate and distinct shoulders created and shown in the red and blue. The shoulders of each "core" must comprise separate lines. This means that they can't be the same obviously.

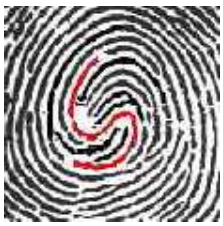
J

K



L

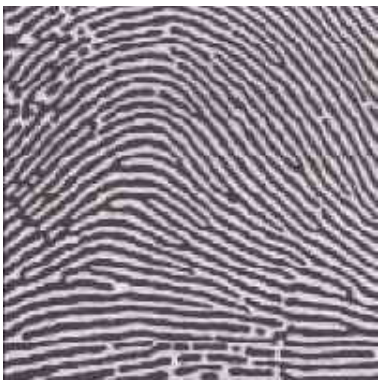
By using a little creative editing I have now changed image L and the way it appears in image M. The significant change is that I have edited this image so that both apparent shoulders (cores) now use the same line (indicated in red). Because they both now use the same line to form the shoulders of each core this is no longer a valid double loop whorl. If there is a problem with identifying a double loop whorl it is probably because of the failure to either identify that there is a separate and distinct shoulder to each core. If the shoulder is formed by the same recurving line then it is not valid. Another issue comes into play and that is if the core or shoulder is actually valid itself.



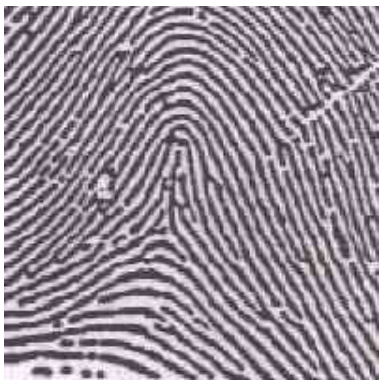
M

-Arches:

Arches represent only about 5 per cent of the fingerprint patterns encountered. In arch patterns, the ridges run from one side to the other of the pattern, making no backward turn. There is ordinarily no delta, but where there is the appearance of a delta, no recurving ridge must intervene between the core and delta points. Arches come in two types, plain or tented. Arches by definition have no delta's. If the pattern has a delta then it is a loop and if it has more than one delta it is a whorl. You will notice in the image at right (plain arch) that there is no delta and no significant core. Because there is no delta this pattern, by default, has to be an arch. If you study the image and look at the overall pattern you notice that the pattern area tends to just flow through the print with no significant changes. This makes it a plain arch pattern. If you compare the two images, plain arch and tented arch, you can see that while the plain arch tends to flow rather easily through the pattern with no significant changes, the tented arch does make a significant change and does not have the same "easy" flow that the plain arch does. The technical definition is that a tented arch has a "significant upthrust" where a plain arch does not. If you study this image long enough you might say "wait there appears to be a delta in there and it can't be an arch with a delta!! Well you are partially correct in that yes, you could see a delta in this print (three sides of the triangle) but here is why it is not a valid delta: To be a valid delta there has to be a significant recurving line which passes in front of the delta, and in this case there is not. In a little simpler terms here is why this can't be a loop, which it would be if it had a valid delta. If you considered the "almost delta" which appears in the near centre left side of the pattern, and you attempted to get a ridge count then the ridge count between the delta and core would be "0". You cannot have a loop with a "0" ridge count. If you call something a loop and then when you try to get a ridge count you come up with "0" then it is not a loop but rather a tented arch, more than likely.



Plain Arch



Tented Arch

So now we know about fingerprints patterns. But how do we match a fingerprint, what are the methods for matching. First let's start by the process of matching.

-The process of matching:

Fingerprint matching consists of five main steps, and they are :

1- Preprocessing.
2- Classification.
3- Minutiae Extraction.
4- Post-Processing.
5- Minutiae Matching.

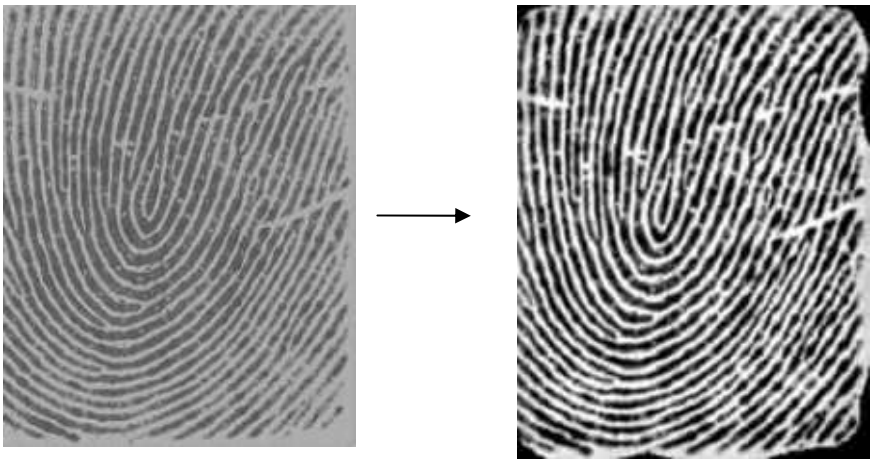
1-Preprocessing:
When a fingerprint image is captured it contains a lot of redundant information. Problems with scars, too dry or too moist fingers, or incorrect pressure must also be overcome to get an acceptable image. Therefore, preprocessing, consisting of enhancement and segmentation is applied to the image. The steps that are present in almost every process are:

1) normalization
2) filtering
3) binarization
4) skeletonization

-Normalization:
To normalize an image is to spread the gray scale in a way that it is spread evenly and fill all available values instead of just a part of the available gray scale. The normal way to plot the distribution of pixels with a certain amount of gray (the intensity) is via a histogram. To be able to normalize an image, the area which is to normalize within, has to be known. Thus it is necessary to find the highest and the lowest pixel value of the current image. Every pixel is then evenly spread out along this scale. The following equation represents the normalization process:

$$I_{norm}(x,y) = \frac{I(x,y) - I_{\min}}{I_{\max} - I_{\min}} \times M$$

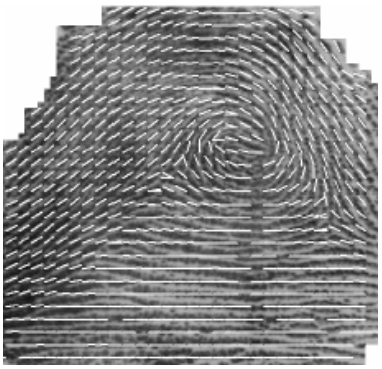
where I is the intensity (gray level) of the image. I_{min} is the lowest pixel value found in the image, I_{max} is the highest one found. M represents the new maximum value of the scale, mostly $M = 255$, resulting in 256 different gray levels, including black (0) and white (255). $I_{norm}(x, y)$ is the normalized value of the pixel with coordinates x and y in the original image $I(x,y)$. When images have been normalized it is much easier to compare and determine quality since the spread now has the same scale. Without the normalization it would not be possible to use a global method for comparing quality.



Raw image from sensor Normalized image

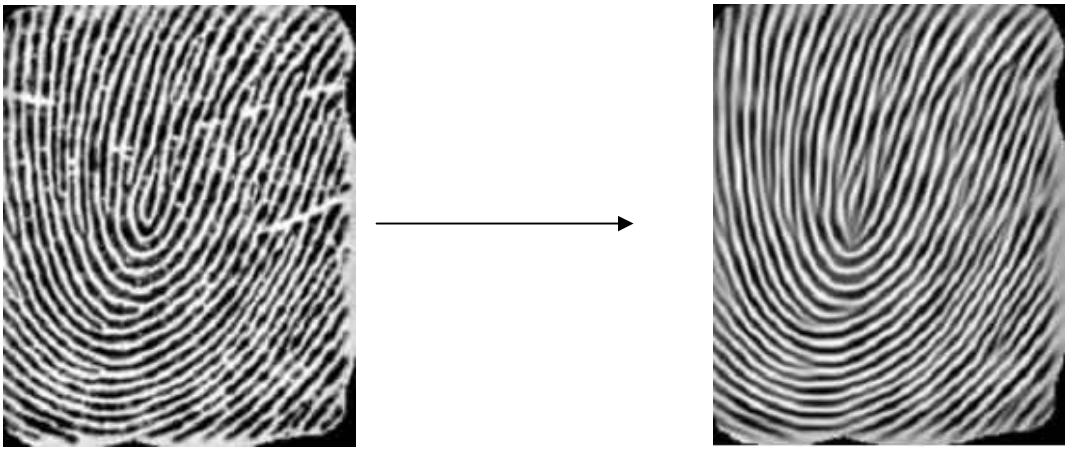
-Filtering:

It is important to filter out image noise coming from finger consistency and sensor noise. For that purpose the orientation of the ridges can be determined so that it is able to filter the image exactly in the direction of the ridges.



An orientation field overlayed on a fingerprint

By this filter method the ridge noise is greatly reduced without affecting the ridge structure itself. One approach to ridge orientation estimation relies on the local image gradient. A gray scale gradient is a vector whose orientation indicates the direction of the steepest change in the gray values and whose magnitude depends upon the amount of change of the gray values in the direction of the gradient. The local orientation in a block can be determined from the pixel gradient orientations of the block.

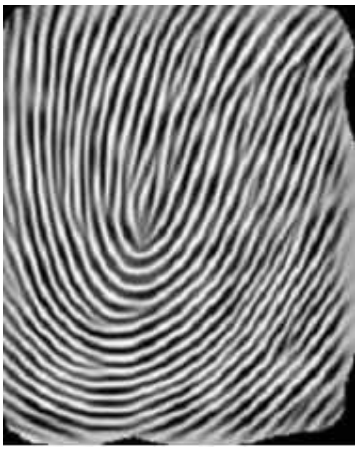


Normalized image

Directionally filtered image

- Binarization:

Binarization can be seen as the separation of the object and background. It turns a gray scale picture into a binary picture. A binary picture has only two different values. The values 0 and 1 are represented by the colors black and white, respectively. To perform binarization on an image, a threshold value in the gray scale image is picked. Everything darker (lower in value) than this threshold value is converted to black and everything lighter (higher in value) is converted to white. This process is performed to facilitate finding identification marks in the fingerprints such as singularity points or minutiae. The difficulty with binarization lies in finding the right threshold value to be able to remove unimportant information and enhance the important one. It is impossible to find a working global threshold value that can be used on every image. The variations can be too large in these types of fingerprint images that the background in one image can be darker than the print in another image. Therefore, algorithms to find the optimal value must be applied separate on each image to get a functional binarization. There are a number of algorithms to perform this, the most simple one uses the mean value or the median of the pixel values in the image. This algorithm is based on global thresholds. What often are used nowadays are local thresholds. The image is separated into smaller parts and threshold values are then calculated for each of these parts. This enables adjustments that are not possible with global calculations. Local thresholds demand a lot more calculations but mostly compensate it with a better result.

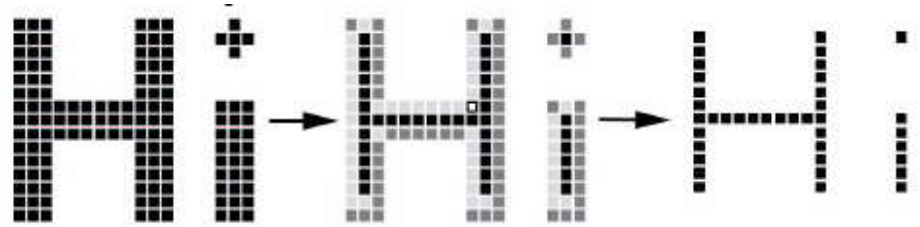


Directionally filtered image

Binarized image

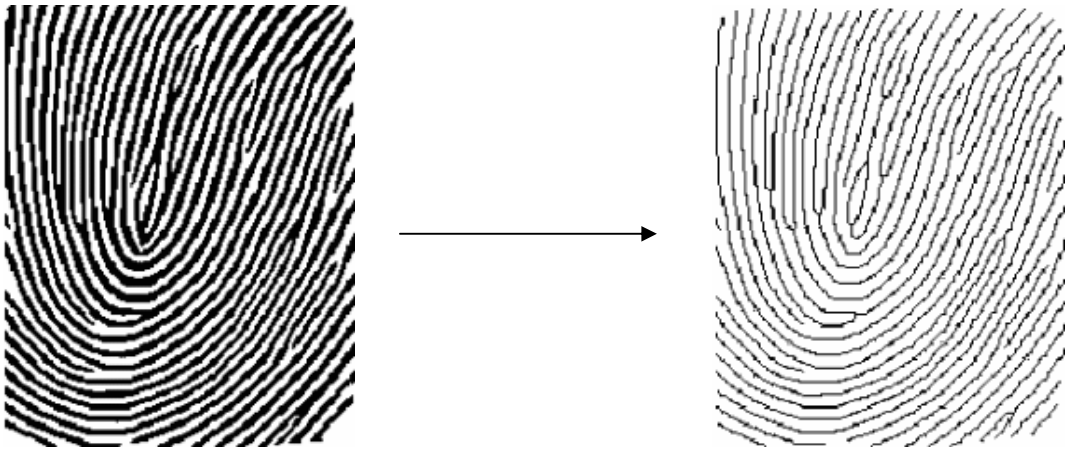
- Skeletonization :

One way to make a skeleton is with thinning algorithms. The technique takes a binary image of a fingerprint and makes the ridges that appear in the print just one pixel wide without changing the overall pattern and leaving gaps in the ridges creating a sort of "skeleton" of the image. The form ✣ is used as structural element, consisting of five blocks that each present a pixel. The pixel in the center of that element is called the origin. When the structural element overlays the object pixels in its entirety, only the pixels of the origin remain. The others are deleted.



An example of skeletonization

Skeleton modeling makes it easier to find minutiae and removes a lot of redundant data, which would have resulted in longer process time and sometimes different results. There are a lot of different algorithms for skeleton modeling that differ slightly.



Binarized image

Skeletonized image

2- Classification:

Classification is based on the fingerprint patterns; we talked about the fingerprint patters some pages ago, so now we will talk about the classification techniques. Several approaches have been developed for automatic fingerprint classification. The best approaches can be broadly categorized into the following categories:

- *Rule-based*

These approaches mainly depend on the number and position of the singular points of the fingerprint. This is the approach commonly used by human experts for manual classification. A plain arch has no singular points. A tented arch, left loop and right loop have one loop and one delta. A whorl has two loops (or a whorl) and two deltas. The result of this technique is a scheme to follow, which tells in which class the input image belongs to.

- *Structural*

Structural approaches are based on the relational organization in the structure of the fingerprints. They are often based on the orientation field.

- *Statistical*

In statistical approaches, a fixed-size numerical feature vector is derived from each fingerprint and a general-purpose statistical classifier is used for the classification. One of the most widely adopted statistical classifiers is the *k*-nearest neighbor. Many approaches directly use the orientation image as a feature vector.

- *Neural network-based*

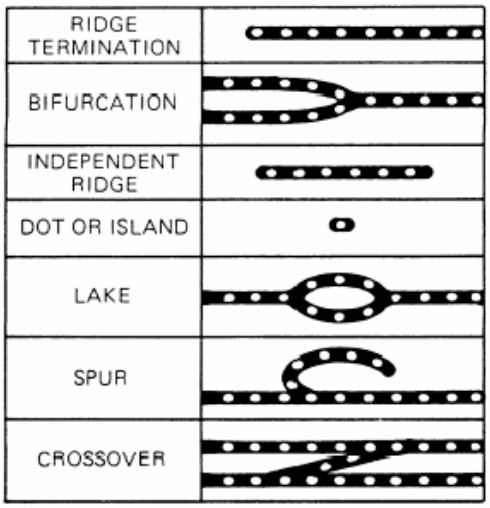
Most of the proposed neural network approaches are based on multilayer perceptrons and use the elements of the orientation image as input features.

- *Multi-classifier*

Different classifiers offer complementary information about the patterns to be classified, which may improve performance.

3- Minutiae Extraction:

At the local level, a total of 150 different local ridge characteristics, called minutiae details, have been identified. Most of them depend heavily on the impression conditions and quality of fingerprints and are rarely observed in fingerprints. The seven most prominent ridge characteristics are shown in following figure:



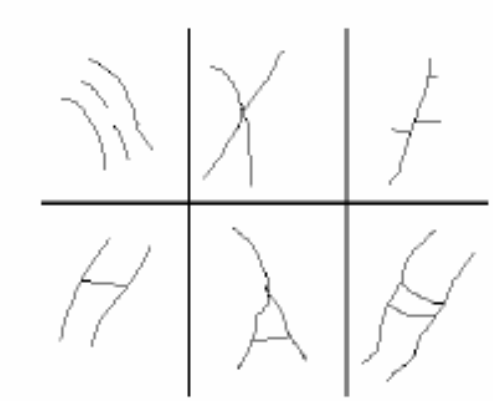
Minutiae details

The measured fingerprint area consists in average of about thirty to sixty minutiae points depending on the finger and on the sensor area. These can be extracted from the image after the image processing step (and possibly the classification step) is performed. 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. Once the thinned ridge map is available, the ridge pixels with three ridge pixel neighbors are identified as ridge bifurcations, and those with one ridge pixel neighbor identified as ridge endings. However, all the minutiae detected are no facts yet because of image processing and the noise in the fingerprint image. For each extracted minutia a couple of features are stored: the absolute position (x,y), the direction (θ), and if necessary the scale (s).
The location of the minutiae are commonly indicated by the distance from the core, with the core serving as the (0,0) on an x,y-axis. Some authors 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. This angle is taken from a horizontal line extending rightward from the core.
At the very fine level, intra-ridge details can be detected. These are essentially the finger sweat pores whose position and shape are considered highly distinctive. However, extracting pores is usable only in high-resolution fingerprint images of good quality and therefore this kind of representation is not practical for most applications.

4- Post-Processing:

Minutiae localization begins with a preprocessed 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, since minutiae are very rarely adjacent. Irregularities caused by scars, sweat or dirt appear as false minutiae, and algorithms locate any points or patterns that do not make sense, such as a spur on an island (probably false) or a ridge crossing at right angles to two or three others (probably a scar or dirt). A large percentage of false minutiae are discarded in this post-processing stage.

In the following figure several examples of false minutiae can be observed. In clockwise order: interrupted ridges, forks, spurs, structure ladders, triangles and bridges are depicted in the figure. The interrupted ridges are two very close lines with the same direction. Two lines connected by a noisy line compose a fork. The spurs are short lines whose direction is orthogonal to ridges direction. The structure ladders are pseudo-rectangle between two ridges. The triangles are formed by a real bifurcation with a noisy line between two ridges. Finally, the bridge is a noisy line between two ridges. All these characteristics generate several false minutiae. The algorithm is divided into several steps, executed in a pre-arranged order: elimination of the spurs, union of the endpoints, elimination of the bridges, elimination of the triangles, elimination of the structure ladders.



False minutiae: interrupted ridges, forks, spurs, structure ladders, triangles and bridges, in clockwise order

5- Minutiae Matching:
Minutiae-based techniques first find minutiae points and then map their relative placement on the finger in order to match the minutiae with the template fingerprint minutiae. Here are 3 general approaches to the algorithms.

-General Approach:

Let T and I be the representation of the template and input fingerprint, respectively. This representation is a feature vector whose elements are the fingerprint minutiae:

$T = \{m_1, m_2, \ldots, m_m\}$
$I = \{m'_1, m'_2, \ldots, m'_n\}$,

where m and n denote the number of minutiae in T and I, respectively.

Each minutia may be described by a number of attributes, including its location in the fingerprint image, orientation, type (e.g. termination or bifurcation), a weight based on the quality of the fingerprint image in the neighborhood of the minutia, and so on. Most common minutiae matching algorithms consider each minutia as a triplet $m = \{x, y, \theta\}$ that indicates the coordinates (x, y) of the absolute location of the minutia and the minutia angle θ:
$m_i = \{x_i, y_i, \theta_i\}$ $\quad i = 1..m$
$m'_j = \{x'_j, y'_j, \theta'_j\}$ $\quad j = 1..n$

A minutia m'_j in I and a minutia m_i in T are considered matching, if the spatial distance between them is smaller than a given tolerance r_0 and the direction difference between them is smaller than an angular tolerance θ_0:
spatial_distance$(m'_j, m_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \le r_0$
and
direction_distance$(m'_j, m_i) = \min\left(\left|\theta'_j - \theta_i\right|, 360^\circ - \left|\theta'_j - \theta_i\right|\right) \le \theta_0$.

This last equation takes the minimum of the two because of the circularity of angles (the difference between angles of 2° and 358° is only 4°). The tolerances r_0 and θ_0 are necessary to compensate for the unavoidable errors made by feature extraction algorithms.

In order to match the fingerprints, there has to be done a displacement and rotation and possibly some other geographical transformations as well. When the fingerprints are from two different scanners, the resolution may vary. So the scale has to be considered. Also the prints can be damaged or affected by distortions. There has to be a mapping function to deal with these problems. See figure 10 for the transformation of a minutia point in two fingerprints.

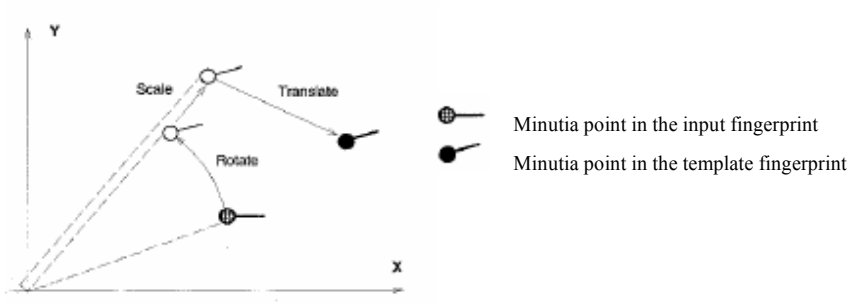


Figure 10 applying a transformation to a minutia point

In the absence of noise and other deformation, the rotation and displacement between two images can be completely determined using two corresponding point pairs. In the ideal scenario, the true alignment can be estimated by testing all possible pairs of minutiae for correspondence and then selecting the best correspondence.

Let map() be the function that maps a minutia m'_j (from I) into m''_j according to a given geometrical transformation. For example, by considering a displacement of $[\Delta x, \Delta y]$, and a counterclockwise rotation θ around the origin:

$$\text{map}_{\Delta x,\Delta y,\theta}(m'_j = \{x'_j, y'_j, \theta'_j\}) = m''_j = \{x''_j, y''_j, \theta'_j + \theta\}, \text{ where}$$

$$\begin{bmatrix} x''_j \\ y''_j \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x'_j \\ y'_j \end{bmatrix} + \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix}.$$

A pair of fingerprints that are most alike will have the maximum number of matching minutiae. Let mm() be an indicator function that returns 1 in the case where the minutiae m''_j and m_i match according to the spatial distance and direction distance:

$$\text{mm}(m''_j, m_i) = \begin{cases} 1 & \text{spatial\_distance}(m''_j, m_i) \le r_0 \quad \text{and} \quad \text{direction\_distance}(m''_j, m_i) \le \theta_0 \\ 0 & \text{otherwise} \end{cases}$$

Then the problem can be formulated as:

$$\max_{\Delta x,\Delta y,\theta,P} \sum_{i=1}^{m} mm(map_{\Delta x,\Delta y,\theta}(m'_{P(i)}), m_i),$$

which indicates the maximum number of matched minutiae. The function P(i) determines the paring between I and T minutiae. In particular, each minutia has either exactly one mate in the other fingerprint or has no mate at all. See figure 11 for an example of pairing. If m_1 were mated with m''_2 (the closest minutia), m_2 would remain unmated. However pairing m_1 with m''_1, allows m_2 to be mated with m''_2, thus maximizing the last equation.

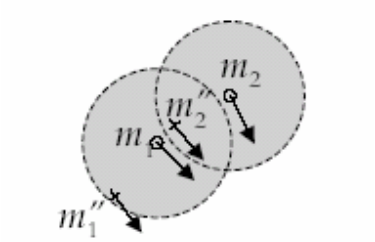


Figure 11: An example of pairing minutiae

- The Hough transform-based algorithm:

Many transformations for minutiae matching are based on the Hough transform-based approach. It is an algorithm with embedded fingerprint alignment in the minutiae matching stage, it discretizes the set of all allowed transformations, and for each transformation, the matching score is computed. The transformation with the maximal score is believed to be the correct one. It consists of three major steps:

1) Estimate the transformation parameters Δx, Δy, θ, and s between the two representations, where Δx and Δy are translations along x- and y-directions, respectively, θ is the rotation angle, and s is the scaling factor.

2) Align the two sets of minutiae points with the estimated parameters and count the matched pairs within a bounding box.

3) Repeat the previous two steps for the set of discretized allowed transformations. The transformation that results in the highest matching score is believed to be the correct one.

The space of transformations consists of quadruples (Δx, Δy, θ, s), where each parameter is discretized (denoted by the symbol +) into a finite set of values:

$\Delta x^+ \in \{\Delta x^+_1, \Delta x^+_2, \ldots, \Delta x^+_a\}$ $\quad\quad$ $\theta^+ \in \{\theta^+_1, \theta^+_2, \ldots, \theta^+_c\}$

$\Delta y^+ \in \{\Delta y^+_1, \Delta y^+_2, \ldots, \Delta y^+_b\}$ $\quad\quad$ $s^+ \in \{s^+_1, s^+_2, \ldots, s^+_d\}$

A four-dimensional array A, with one entry for each of the parameter discretizations, is initially reset and the following algorithm is executed:

```
For each m_i, i = 1..m                          //for each template minutia point
For each m'_j, j = 1..n                         //for each input minutia point
For each θ+ ∈ {θ+1, θ+2, …, θ+c}                //for each discretized rotation
  If direction_distance(θ'j + θ+, θi) < θ0      //if the directions difference //after rotation is small
    For each s+ ∈ {s+1, s+2, …, s+d}            //for each discretized scale
    {
     [Δx; Δy] = [xi; yi] − s+ [cos θ+  −sin θ+; sin θ+  cos θ+] [x'j; y'j]   //compute displacement
     Δx+, Δy+ = quantization of Δx, Δy to the nearest bin
     A[Δx+, Δy+, θ+, s+] = A[Δx+, Δy+, θ+, s+] + 1
                                                //count matched pairs
    }
}}}
(Δx*, Δy*, θ*, s*) = arg max A[Δx+, Δy+, θ+, s+]
//where the count of matched pairs is highest, give the optimal displacement, rotation and scale
```

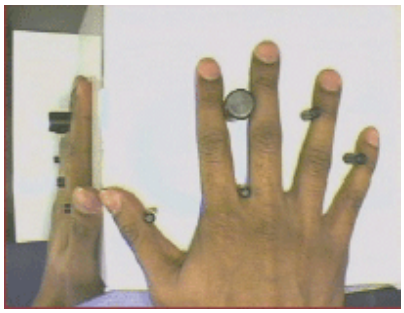
This maximum gives the transformation that is believed to be the right one. If there exists a matching fingerprint in the database, the template with the most matching minutiae is probably the same as the input.

- Pre-alignment:

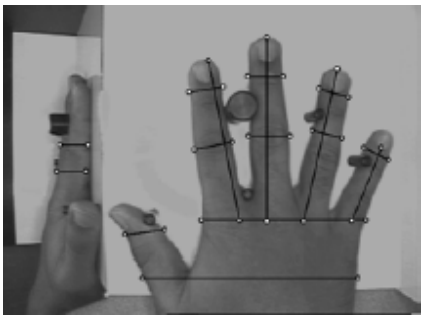
An intuitive more logical choice would be to pre-align all the templates in the database and the input image before the matching procedure. In this way the alignment takes place only once for every image. A great advantage is that it significantly reduces the computational time. Pre-alignment cannot compare images to one another so only depends on the properties of itself. The most common pre-alignment technique convert the fingerprint according to the position of the core point. Unfortunately, reliable detection of the core is very difficult in noisy images and in arch type patterns. For adjusting the rotation the shape of the silhouette, the orientation of the core delta segment, the average orientation in some regions around the core, and the orientations of the singularities can be used. But still this is a complex problem and causes often errors in the matching procedure. That is the main reason why embedded alignment in the minutiae matching stage is often used.

4.7 Hand Geometry:

The concept of using hand geometry is measuring and recording the length, width, thickness, and surface area of the hand while guided on a plate. The image captures both the top surface of the hand and a side image that is captured using an angled mirror. After capturing the silhouette image 31,000 are analyzed and 90 measurements are taken; the measurements range from the length of the fingers to the distance between the knuckles, this information is stored in nine bytes of data.



Hand including mirror image
As seen by the CCD camera

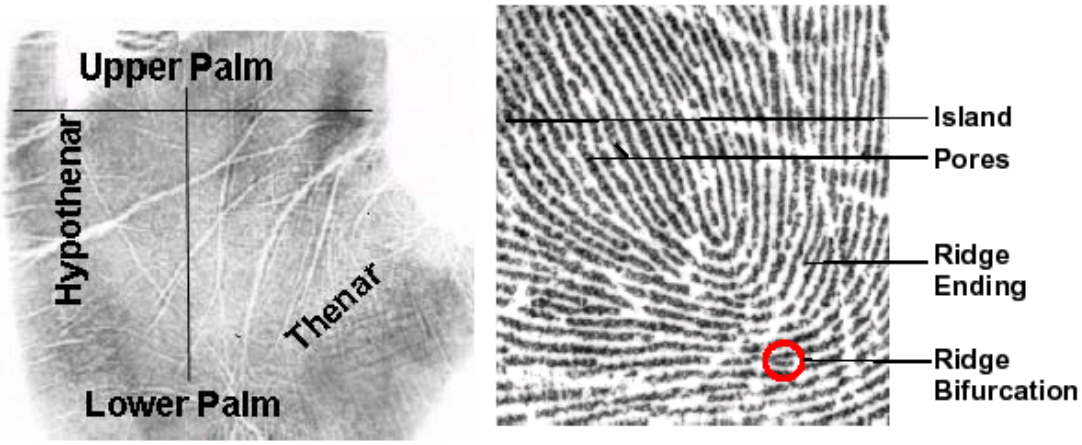


Example distance measurement

The enrollment process of a hand geometry system requires the capture of three sequential images of the hand, which are evaluated and measured to create a template of the person's characteristics.

4.8 Palmprint:

Palmprint is based on the aggregate of information presented in a friction ridge impression. This information includes the flow of the friction ridges (Level 1 Detail), the presence or absence of features along the individual friction ridge paths and their sequences (Level 2 Detail), and the intricate detail of a single ridge (Level 3 detail).
A palm
recognition system is designed to interpret the flow of the overall ridges to assign a classification and then extract the minutiae detail — a subset of the total amount of information available, yet enough information to effectively search a large repository of palm prints. Minutiae are limited to the location, direction, and orientation of the ridge endings and bifurcations (splits) along a ridge path. The images in Figure 12 present a pictorial representation of the regions of the palm, two types of minutiae, and examples of other detailed characteristics used during the automatic classification and minutiae extraction processes.



the three main categories of palm matching techniques are minutiae-based matching, correlation-based matching, and ridge-based matching. Minutiae-based matching,
the most widely used technique, relies on the minutiae points, specifically the location, direction, and orientation of each point. Correlation-based matching involves simply lining up the palm images and subtracting them to determine if the ridges in the two palm images correspond. Ridgebased matching uses ridge pattern landmark features such as sweat pores, spatial attributes, and geometric characteristics of the ridges, and/or local texture analysis, all of which are alternates to minutiae characteristic extraction. Minutiaebased matching typically attains higher recognition accuracy, although it performs poorly with low quality images and does not take advantage of textural or visual features of the palm. Processing using minutiae-based techniques may also be time consuming because of the time associated with minutiae extraction. Correlation-based matching is often quicker to process but is less tolerant to elastic, rotational, and

translational variances and noise within the image. Some ridge-based matching characteristics are unstable or require a high-resolution sensor to obtain quality images. The distinctiveness of the ridge-based characteristics is significantly lower than the minutiae characteristics.

4.9 Signature:

"Dynamic Signature" is a biometric modality that uses, for recognition purposes, the anatomic and behavioral characteristics that an individual exhibits when signing his or her name (or other phrase). Dynamic signature recognition uses multiple characteristics in the analysis of an individual's handwriting. These characteristics vary in use and importance from vendor to vendor and are collected using contact sensitive technologies, such as PDAs or digitizing tablets. Signature identification systems analyze two different areas of an individual's signature:

1- Specific feature of the signature.
2- Specific features of the process of signing.

The features that are taken into account and measure include speed, pen pressure, directions, stroke length, and when the pen is lifted from the paper. These devices store these factors for future comparisons in their database. Signature identification devices also can analyze the "static" image of one's signature, which captures the entire image of one's signature and stores it for comparison. These devices account for changes in one's signature over time by recording the time, history of pressure, velocity, location, and acceleration of a pen each time a person uses the system.

Figure 12 Dynamic Signature Depiction: As an individual signs the contact sensitive tablet, various measurements are observed and processed for comparison.

Common dynamic characteristics include the velocity, acceleration, timing, pressure, and direction of the signature strokes, all analyzed in the X, Y, and Z directions. Figure 13 illustrates these recorded dynamic characteristics of a signature. The X and Y position are used to show the changes in velocity in the respective directions (indicated by the white and yellow lines) while the Z direction (red line) is used to indicate changes in pressure with respect to time.

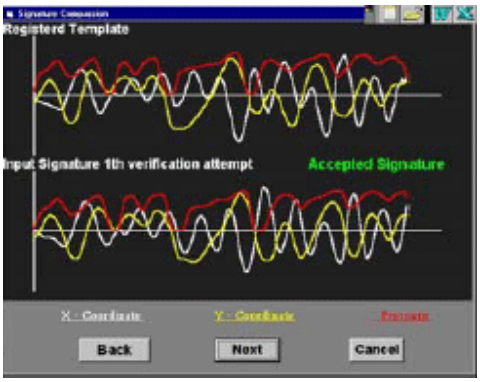


Figure 13 - Graphic Depiction of Dynamic Signature Characteristics.

Some dynamic signature recognition algorithms incorporate a learning function to account for the natural changes or drifts that occur in an individual's signature over time. The characteristics used for dynamic signature recognition are almost impossible to replicate. Unlike a graphical image of the signature, which can be replicated by a trained human forger, a computer manipulation, or a photocopy, dynamic characteristics? are complex and unique to the handwriting style of the individual. Despite this major strength of dynamic signature recognition, the characteristics historically have a large intra-class variability (meaning that an individual's own signature may vary from collection to collection), often making dynamic signature recognition difficult.

4.10 Keystroke dynamics:

Keystroke dynamics is a biometric based on assumption that different people type in uniquely characteristic manners. Observation of telegraph operators in the 19th century revealed personally distinctive patterns when keying messages over telegraph lines, and telegraph operators could recognize each other based on only their keying dynamics. Conceptually closest correspondence among biometric identification systems is signature recognition. In both signature recognition and keystroke dynamics the person is identified by their writing dynamics which are assumed to be unique to a large degree among different people. Keystroke dynamics is known with a few different names: keyboard dynamics, keystroke analysis, typing biometrics and typing rhythms. Keystroke dynamics is mostly applicable to verification, but also identification is possible. In verification it is known who the user is supposed to be and the biometric system should verify if the user is who he claims to be. In identification, the biometric system should identify the user without any additional knowledge, using only keystroke dynamics. Most applications of keystroke dynamics are in field of verification.

- Features used with keystroke dynamics:
Keystroke dynamics include several different measurements which can be detected when the user presses keys in the keyboard, Possible measurements include:

– Latency between consecutive keystrokes.
– Duration of the keystroke, hold-time.
– Overall typing speed.
– Frequency of errors (how often the user has to use backspace).
– The habit of using additional keys in the keyboard, for example writing numbers with the numpad
– In what order does the user press keys when writing capital letters, is shift or the letter key released first.
– The force used when hitting keys while typing (requires a special keyboard).
Statistics can be either global, i.e, combined for all keys, or they can be gathered for every key or keystroke separately. Systems do not necessarily employ all of these features. Most of the applications measure only latencies between consecutive keystrokes or durations of keystrokes. In figure 14 is an example of writing word “password” several times and measuring latencies between keystrokes. Timings have been measured for three different persons. There are clear differences in latencies and their standard deviations.

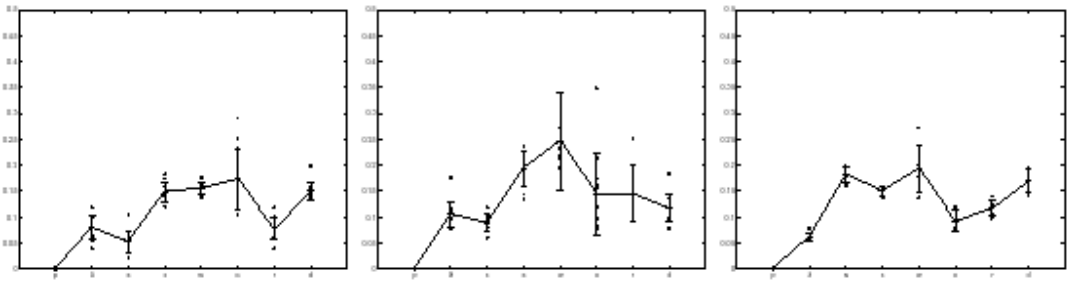


Figure 14 - Latencies between keystrokes when writing word “password” by three different persons. The word was written several times. The lines represent average latencies, errorbars represent standard deviations.

Latencies between keystrokes and durations of keystrokes are popular measurements because they can be easily measured with normal PC hardware. Both key press and release events generate hardware interrupts. Gathering keystroke dynamics data has, however, few complications. Several keys can be pressed at the same time – the user presses the next key before releasing the previous one and it happens quite often when writing fast. Depending on what is measured, there might even be negative time between releasing a key and pressing the next. It also adds slightly to complexity of the keystroke dynamics system if it is wanted to know when the user presses SHIFT, ALT and other special keys. Another challenge is that there is a very wide variety of typing skills, and the biometric systems should work for all users. First of all, the speed of typing can be wildly different between different users. An experienced touch-typist writes easily several tens of times faster than a beginner using “hunt-and-peck” style with one finger. Also the predictability of a fast writer is much greater – there is no need to stop and think where some letter is located on the keyboard. The typing can also be affected if the user is on a lower level of alertness, for example sleepy or ill. Users will additionally sometimes have accidents and consequently write in an ab-normal fashion for a few weeks when a finger is bandaged, or type with one hand when holding a coffee cup in other hand, and so on. Changing keyboard to a different model or using a laptop computer instead of a normal PC can also affect keystroke dynamics tremendously. All these factors have to be taken into account when designing a keystroke dynamics system.

4.11 Gait:

Gait recognition is a relatively new research direction. It aims to seek distinguishable variations between the same actions of walking from different people for the purpose of automatic identity verification. Given the ability of humans to identify persons and classify gender by the gait of a walking subject, there have been a few computer vision algorithms developed for people identification and activity classification. Cutler and Davis used self-correlation of moving foreground objects to distinguish walking humans from other moving objects such as cars. Polana and Nelson detected periodicity in optical flow and used these to recognize activities such as frogs jumping and human walking. Bobick used a time delayed motion template to classify activities. Little and Boyd used moment features and periodicity of foreground silhouettes and optical flow to identify walkers. Nixon used principal component analysis of images of a walking person to identify the walker by gait.

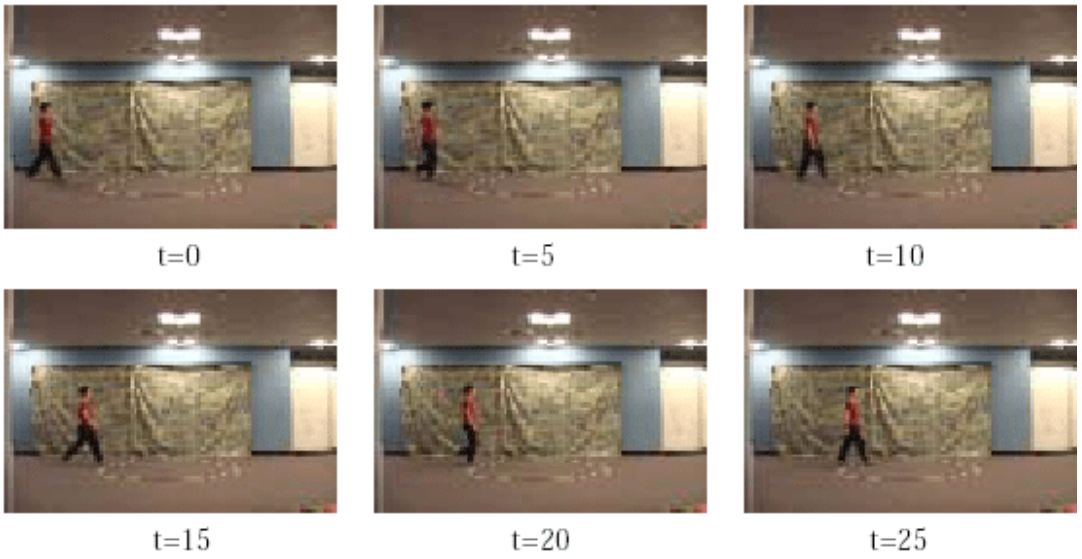


Figure 15 - An example sequence of a walking person.

4.12 Odor:

Olfaction has an extremely high importance in the human being. It is one of the five main senses. Many philosophers and scientists has been trying to comprehend the sense of the smell for several thousand years. It is difficult task, because people often have problem with finding words even to describe their smell sensations. However, odorants influence deeply our life, mood. Reactions like discomfort, attraction, and etc. sensation are hard to extinguish since neurons of the nose are connected straight to a part of the brain, so-called olfactory bulb, and the olfaction mechanism is still unknown.
Anything that has an odor constantly evaporates tiny quantities of molecules that produce the smell, so-called odorants. A sensor that is capable to detect these molecules is called a chemical sensor. In this way the human nose is a chemical sensor and the smell is a chemical sense. The human's ability to smell is not so perfect in comparison with animals. human brain devotes only 4,8 cm2 to the entire olfactory apparatus At the same time a dog uses 65 cm2 and a shark utilizes 2,3 m2. Despite of its inferiority, a human has about 40 million olfactory nerves. This allows detecting even slight traces of some chemical components. Some odorants can be detected even if the concentration in the air is only one part per trillion. Odor information processing in human model is tremendously complicated task. It has been discussed in a huge amount of works. Humanity knows much about the functional characteristics and structure of the brain and can comprehend at least some of its information processing mechanisms. However, overall dynamical properties of the brain are still unknown. If we can catch the behavior of the olfactory system it can be helpful to understand how other parts are involved. Diversity of different methods has been used to understand olfaction. The most exciting methods have been proposed by Freeman. He has shown that in the olfactory bulbs each neuron participates in the generation of olfactory perception and no one receptor type alone identifies a specific odor. Main operations of olfaction can be divided roughly in five parts: sniffing, reception, detection, recognition, and cleansing. The olfaction begins with sniffing that mixes the odorants into a uniform concentration and delivers these mixtures to the mucus layer in the upper part of nasal cavity. Next these molecules are dissolved in this layer and transported to the cilia of the olfactory receptor neurons. Reception process includes binding of these odorant molecules to the olfactory receptors. Odorant molecules are binded temporarily to proteins that transport molecules across the receptor membrane with simultaneous stimulation of the receptors. During this stimulation the chemical reaction produces an electrical stimulus. These electrical signals from the receptor neurons are transported to the olfactory bulb. From the olfactory bulb the receptor response information is forwarded to the olfactory cortex (detection). Odor recognition part takes place namely in the olfactory cortex. Then the information is transmitted to the cerebral cortex. Remind that there are no individual receptors or parts of the brain capable to recognize specific odors. The brain is key component associated the collection of olfactory signals with the specific odor. Cleansing finishes the olfaction process. For this purpose the breathing fresh air removing of odorant molecules from the olfactory receptors is required.

To grasp the mechanism of olfactory perception the model of our nose can be considered. The schematic view on the human nose is presented in Figure 16.

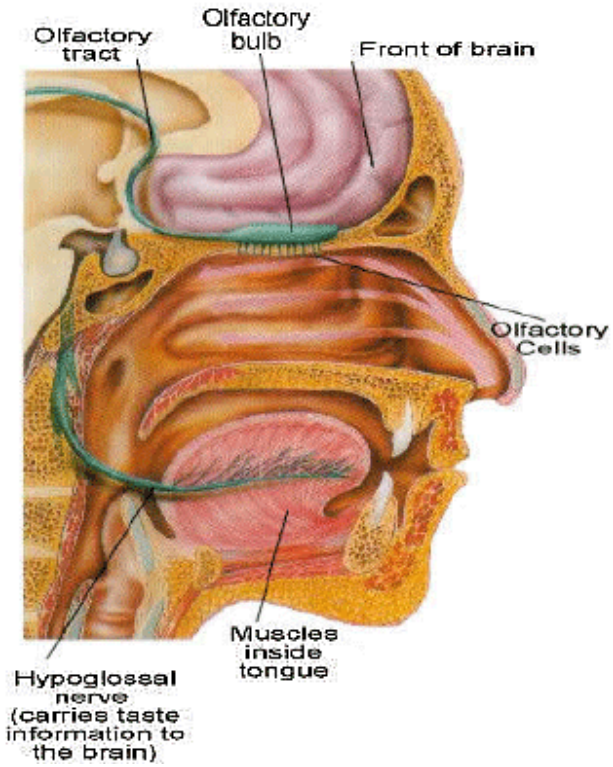


Figure 16 Human Olfactory Model.

As it follows from Figure 16 inside each side of the nose is an air chamber, the nasal cavity. Air including odorants inhaled through the nostril and flows down. During the sniffing, air swirls up into the top of the cavity. Here is a small patch of about 10 million specialized olfactory cells. They have long micro-hairs, or cilia, sticking out from them. Odor particles in the air stick on to the cilia and make the olfactory cells produce nerve signals, which travel to the olfactory bulb. This is a pre-processing centre that partly sorts the signals before they go along the olfactory tract to the brain where they are recognized as smells.

- Electronic Olfactory Model:

Remind that the main task in odor recognition to create a model as similar to the human model as it is possible. From this point of view electronic/artificial noses (socalled ENoses) are being developed as a system for the automated detection and classification of odors, vapors, gases. ENose is represented as a combination of two components: sensing system and pattern recognition system. The schematic representation of ENose can be found in Figure 17.

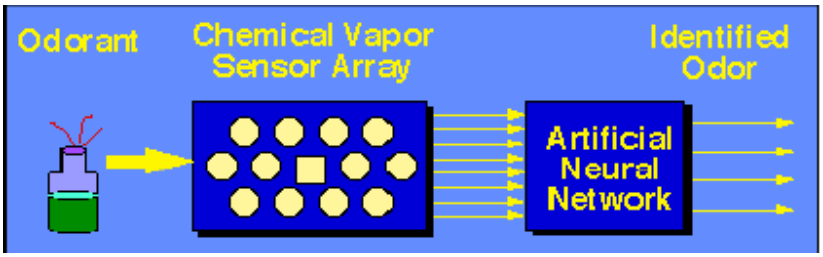


Figure 17 - Schematic Diagram of ENose.

Sensing system is represented as an array of chemical sensors where each sensor measures a different property of the sensed chemical, or as a single sensing device or as a hybrid of both. The major task of this component is to catch the odor. Each odorant presented to the sensing system produces a signature of characteristic pattern of the odorant. Database of signatures is built up by presenting many different odorants to the sensing system. It is used further to create the odor recognition system.
Pattern recognition system is utilized to recognize procedure. The goal of this process is to train and create the recognition system that will be capable to produce unique classification or clustering of each odorants so that an automated identification can be implemented. This process incorporates several approaches: Statistical, ANN, Neuromorphic.

- Sensing System:

Sensing system allows tracing the odor from the environment. This system can be single sensing device, like gas chromatograph, spectrometer, In this case it produces an array of measurements for each component. The second type of sensing system is an array of chemical sensors. It is more appropriate for complicative mixtures because each sensor measure a different property of the sensed chemical. Hybrid of single sensing device and array of chemical sensors is also possible. Each odorant presented to the sensing system produces a characteristic pattern of the odorant. By presenting a mass of sundry odorants to this system a database of patterns is built up. It is used then to construct the odor recognition system. There are 5 available categories of sensors:

1-Conductivity Sensors:
There are two types of conductivity sensors: metal oxide and polymer. They exhibit a change in resistance when exposed to volatile organic compounds. Both these classes are widely available commercially because of its low cost. These sensors respond to water vapor, humidity difference, but not too sensitive for specific odorants.
Conducting polymer sensors are commonly used in electronic nose systems. Because conducting polymer sensors operate at ambient temperature, they do not need heaters and thus are easier to make. The electronic interface is straightforward, and they are suitable for portable instruments.

2-Piezoelectric Sensors:
The piezoelectric family of sensors (quartz crystal microbalance, surface acoustic wave devices) can measure temperature, mass changes, pressure, force, and acceleration. During an operation, a gas sample is adsorbed at the surface of the polymer, increasing the mass of the disk-polymer device and thereby reducing the resonance frequency. The reduction is inversely proportional to odorant mass adsorbed by the polymer. In the electronic nose, these sensors are configured as mass-change-sensing devices.

3-Metal-oxide-silicon field-effect-transistor (MOSFET):
MOSFET odor-sensing devices are based on the principle that volatile odor components in contact with a catalytic metal can produce a reaction in the metal. The reaction's products can diffuse through the gate of a MOSFET to change the electrical properties of the device. Operating the device at different temperatures and varying the type and thickness of the metal oxide the sensitivity and selectivity can be optimized.

4-Optical Fiber Sensors:
Optical-fiber sensors utilize glass fibers with a thin chemically active material coating on their slides or ends. A light source at a single frequency (or at a narrow band of frequencies) is used to interrogate the active material, which in turn responds with a change in color to the presence of the odorant to be detected and measured. Arrays of these devices with different dye mixtures can be used as sensors for an ENose. The main application for such kind of ENoses is medicine.

5-Spectrometry-Based Sensors:
Spectrometry-Based sensors use the principle that each molecular has a distinct infrared spectrum. Usually devices based on theses sensors are quite big and expensive.

-Pattern Recognition System:

Pattern recognition system is the second component of electronic nose used for odor recognition. Its goal is to train or to build the recognition system to produce unique classification or clustering of each odorant through the automated identification. Recognition process incorporates several approaches: Statistical, ANN, Neuromorphic. Many of the statistical techniques are complementary to ANNs and are often combined with them to produce classifiers and clusters. It includes PCA, partial least squares, discriminant and cluster analysis. PCA breaks apart data into linear combinations of orthogonal vectors based on axes that maximize variance. To reduce the amount of data, only the axes with large variances are kept in the representation.
When an ANN is combined with the sensor array, the number of detectable chemicals is generally greater than the number of unique sensor types. A supervised approach involves training a pattern classifier to relate sensor values to specific odor labels. An unsupervised algorithm does not require predetermined odor classes for training. It essentially performs clustering of the data into similar groups based on the measured attributes or features.
Neuromorphic approaches center on building models of olfaction based on biology and implementing them in electronics. Unfortunately, there is a lack of realistic mathematical models of biological olfaction. Thus the area of neuromorphic models of the olfactory system lags behind vision, auditory, motor control models. Olfactory information processed in both the olfactory bulb and in the olfactory cortex. The olfactory bulb performs the signal preprocessing of olfactory information including recording, remapping and signal compression. The olfactory cortex performs pattern classification and recognition of the sensed odors. There are two competing models of olfactory coding. The selective receptor comes from recent experimental results in molecular biology. It can be thought of as an odor mapper. This approach is similar to visual system with the idea of receptive fields of olfactory receptors and mitral cells in the olfactory bulb. The second approach is a non-selective receptor, distributive-coding model that comes from data collected by electrophysiology and imaging of the olfactory bulbs. Neuromorphic approach has an advanced feature consisting in incorporation of temporal dynamics to handle identification of combinations of odors.

4.13 Comparison of Biometric Technologies:

Comparison of Biometric Technologies							
Biometrics	Univer-sality	Unique-ness	Perma-nence	Collect-ability	Perfor-mance	Accept-ability	Circum-vention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H

H=High, M=Medium, L=Low

6. Biometric Security Concerns:

Many of the questions raised about the use of biometrics, particularly in connection with authentication, relate to the trust that can be placed in the biometric authentication process itself, or to the protection of the biometric data that is used by the system and which is private and personal to the users. The aim of this document is to explore these issues in more detail, highlighting a number of commonly expressed security concerns, discussing the possible threats that they pose, and what can be done to eliminate or at least mitigate them. Note that this document does **not** address the details of biometric technical security features and countermeasures.

5.1 - Performance limitations:

Biometrics do not provide perfect (unique) identification. The matching process is probabilistic and is subject to statistical error. A mistaken identification or verification where the wrong person is matched against an enrolled user is termed a False Acceptance and the rate at which these occur is the False Acceptance Rate (FAR). Conversely, an error that occurs where a legitimate user fails to be recognized is termed a False Rejection and the corresponding rate is the False Rejection Rate (FRR). These errors are dependent not only on the technology but also on the application and the environment of use.

Note that FAR and FRR errors are influenœd by numerous factors including: Uniqueness of biometric features :

- Uniqueness of biometric features.
- Capture device.
- Algorithm.
- Environmental interference.
- User population.
- User behavior.

Both FAR and FRR errors may have security implications, the relevance of which will depend on the application.

5.2 - Enrolment integrity:

Ensuring enrolment integrity is a vital underlying requirement for all authentication systems whether or not biometrics are used. If the enrolment integrity is compromised, all bets are off regarding security. System implementers will need to determine what credentials are necessary and sufficient to validate users prior to enrolment, and then to ensure that the enrolment process itself is secure – in most cases this will mean supervision by trusted trained staff.

5.3 - Enrolment quality:

The performance of biometric systems is dependent on the quality of the enrolled biometric. Enrolment quality can be affected by accidental or deliberate events and environmental conditions, and the result of low enrolment quality is almost inevitably poor system performance. If the performance is poor the security will be compromised, and there may be excessive dependence on the fallback system.
In the case of negative ID systems, poor enrolment quality will make it more likely that attempts to establish multiple identities will be successful, because biometrics that should match and trigger an alarm may in practice not do so. This is a direct security concern as it may undermine the principal intended functionality of the system. In the case of positive ID systems, the false rejection rate will be adversely affected which may not be an immediate security concern. However, if this leads to an adjustment of the threshold to make the system work acceptably, the false acceptance rate will, in consequence, also be affected.

5.4 - Spoofing (physiological biometrics):

Spoofing through the use of artefacts is generally a concern for physiological biometric technologies such as fingerprint, hand, iris etc. Several studies dating from around 1998 have demonstrated the potential for successfully mounting a spoofing attack under carefully controlled conditions. If spoofing attacks can be successful, the fundamental tenet of biometrics – the "something you are" – is undermined. Spoofing involves 2 stages: a) - the capture of a biometric "image" belonging to an enrolled user, and b) - transferring the biometric image onto an artefact.

Some features will be more difficult to observe and capture than others, and the skill needed to create a successful artefact will be dependent on both the biometric feature and how resistant the system is to artefacts. Faces are easily captured by photography. Fingerprint patterns may be captured through the lifting of latent or residual images left on smooth surfaces. Voices may be captured on tape or other audio recorder. Some biometric images will be difficult to capture, e.g. retinal patterns, without the use of sophisticated and conspicuous equipment. Of course, given cooperation by the legitimate user, the capturing of biometric features is likely to be much easier.

5.5 - Mimicry (behavioral biometrics):

Mimicry is to behavioral biometrics what artefacts are to physiological biometrics. Through mimicry, an impostor attempts to “copy” the relevant biometric features of an enrolled user in order to fool the biometric authentication process. Because behavioral biometrics are applicable to the recognition of acquired, rather than inherited features, the features can also be acquired by an impostor.

The consequences of successful use of mimicry are likely to be the same as for spoofing previously) for given applications. Impostors are unlikely to attempt mimicry attacks against biometric systems that completely or predominately utilize physiological features (e.g. fingerprint, iris). Because mimicry may be perceived to be a low technology form of attack requiring a lower level of expertise, biometric systems employing behavioral biometrics may be subject to a higher incidence of attacks from a wider range of attackers.

5.6 - Latent/Residual images:

Latency or residual images are a possible security concern that could occur in 2 forms:

- Physical residual biometric image.
- Latency in internal memory.

7-Template integrity/confidentiality:

Template integrity and confidentiality are distinctly different issues related to template data though similar solutions may be employed to deal with both problems. Template integrity is concerned with threats to the authentication process caused by planted or modified templates, whereas template confidentiality relates to the legal and privacy issues around the template data and the way in which the data could be misused.

Integrity:
The integrity of the authentication process depends, among other factors, on the integrity of the template. If either the reference template or the “live” biometric sample is untrustworthy, the resulting authentication will be untrustworthy. Untrustworthy templates could occur for one or more of several different reasons:

- Accidental corruption due to a malfunction of the system hardware or software.
- Intentional modification of a bona-fide template by an attacker.
- The insertion of a biometric template corresponding to the attacker to substitute for the reference template of an authorized enrollee.
- The addition of a biometric template corresponding to the attacker to create a bogus "enrolment" on the system
- The substitution of a biometric sample corresponding to that of an authorized enrollee in place of the live sample of the attacker.

Confidentiality:
Biometric templates contain data that can be used to identify living persons. This means that their processing and storage on a biometric system are subject to legal constraints imposed by the European Data Protection Directive and its enactment in national legislation (the 1998 Data Protection Act in the UK). Other regulatory mechanisms (e.g. Human Rights Act and Health and Safety legislation) may also be relevant. The primary concern is the privacy and protection of personal data and biometric applications will need to include adequate protection to comply with the legal requirements. It should also be noted that other stored or processed biometric data is also subject to legal constraint, e.g. biometric images.

5.8 - Capture/replay attacks:

Capture/replay is the name given to attacks where the biometric signals from an enrolled user are captured at one place and time and replayed later (usually at the same place) in an attempt to fool the system that the enrolled used is present. Although this can arguably occur at many points in the biometric system, the terminology usually applies to electrical signals captured between the capture device and the rest of the system. It may be a particular problem where there is a large and unsupervised path between the 2 components such as a network connection.

5.9 - Biometrics do not provide absolute identification:

Biometric systems can, at best, only identify/verify individuals who have been previously enrolled. Applications can use this functionality in various ways, for example to provide an alert when a stranger is detected (i.e. biometric features captured that do not correspond to an enrolled user). The feasibility and effectiveness of the application will depend on the technology, environment and other details of the implementation. Biometric authentication only addresses part of the overall authentication framework. Non-biometric elements (pre-enrolment) are needed to establish absolute identity with the assurance standards needed for the application using acceptable credentials (e.g. birth certificate, peer endorsement etc).

5.10 - Biometrics are not secret:

Valuable assets are traditionally protected by secrecy, typically secret passwords. Biometric features are often readily observed and do not possess equivalent secrecy. They may also be captured with varying degrees of difficulty.
This is a variation on the spoofing concern. It is certainly true that the source biometric features are not secret, but the argument as expressed is based on an incorrect premise. In fact, biometric security does not depend on the secrecy of the basic biometric features (people readily rely on biometric identification in its human form in day-to-day use). Rather, it depends on the integrity of the authentication mechanism which, in the context of issue raised here, translates into the difficulty of capturing the biometric features of a target and then constructing an artefact that will spoof the system. This can be contrasted with a password which, once disclosed, is trivial to exploit.

5.11 - Biometrics are not random enough:

People are rather alike, and lack the true randomness that passwords can have. Lack of randomness means that it is harder to separate individuals by their characteristics and is easier to confuse them. This is a concern that is hard to refute by theoretical analysis. In fact template sizes are usually much larger than password lengths, though this hardly constitutes a valid argument. Current knowledge of biometric algorithm behavior and human feature randomness and variation does not permit theoretical analysis of biometric system performance.
The pragmatic approach is to use performance testing to explore the interaction of the human and system parameters and thence to determine the discrimination capability of the biometric system. The results are typically expressed in terms of statistical error rates such as FAR and FRR.

5.12 - Biometric algorithms are proprietary and not validated:

Many encryption algorithms are publicly available to allow cryptographers to analyze and verify the strength of the encryption. Biometric algorithms are not readily available for review and are thus an unknown factor. Biometric algorithms do not generally fulfil the same purpose as cryptographic algorithms. Rather, they represent the encoding rules for the biometric feature set to derive a template in order to provide a means of distinguishing between the features of enrolled users of the system. The purpose of the biometric algorithm is functional rather than security related, though there may be security connotations.
If an analyst (or an attacker) wishes to understand the working of the algorithm, then the task is likely to be easier if the algorithm is publicly available. An impostor might wish to examine the algorithm to determine how the biometric ? Template mapping works, and what elements are more and less important to the authentication process. This knowledge could aid the construction of an artefact intended to spoof the system,

particularly if the approach was to be that of an artificially constructed image rather than a copy of a known legitimate image. An undisclosed algorithm would make this process more difficult (security through obscurity) but is unlikely to resist a determined attack that might involve reverse engineering of the algorithm. Conversely, a publicly available algorithm may help to highlight potential weaknesses and thereby assist in their eradication (i.e. as for the case of password algorithms).

5.13 - Biometrics cannot be changed when compromised:

It is true that the basic biometric features cannot be changed, though in some cases, alternatives may be available (e.g. different fingers). However the simplicity of the headline argument conceals some more complex and subtle issues. We need to understand what can be compromised, examine a number of scenarios where compromise might occur and identify what measures may be taken to counter them.

Compromise through use of an artifact:
Here we are referring to the exploitation of the source biometric feature (which is generally not secret anyway) through the capture of the feature and the construction of an artefact with similar characteristics. The 2 issues are:

- How easy is it to capture the features?
- How easy is it to construct an artefact that can spoof the biometric system?

If successful; then, at a minimum, that user on that system is compromised. But the situation is actually worse than that, because once the system has been shown to be vulnerable to spoofing, every enrolled user is at risk of compromise in the same way. Re-enrolling the compromised user (using an alternate feature if available) will not resolve the fundamental problem. Other biometric systems using the same technology may also be vulnerable, which further increases the scope of the potential problem.

Compromise through capture/replay:
If undetected, this attack may be used repeatedly and will compromise that user on that system. However, once in place, other users on the compromised connection may also be captured and the compromised set of users is liable to grow. Once discovered, the attack may be disabled for all compromised users, provided that the capture devices can be protected in future from similar attacks.

5.14 - Biometrics do not offer non-repudiation:

The question of the repudiation of biometrically authenticated transactions has been the subject of widespread discussion. Such discussion is not limited to biometric authentication though; other more traditional forms are also open to debate. Generally, signatures have been accepted as legally binding indicators but they are certainly open to challenge in the courts and such challenges are not unknown.

Non-repudiation of authentication typically rests on 2 considerations:

- Strength of binding of the authenticator to the individual in question
- Informed consent of the individual at the time the authentication was given.

Most authenticators are open to challenge on either or both of these grounds. The former is a technical issue, signifying the non-forgeability (or otherwise) of the authenticator. Normal signatures are known to be readily forgeable, so do not offer strong binding. Various other authentication tokens have been proposed and used which themselves offer much stronger binding, for example cryptographic signatures. However, cryptography does not address the crucial issue of binding the authentication to an individual. This final step has to be provided by a supplementary mechanism usually involving a PIN or password, a token, a biometric, singly or in combination. These generally have much lower strengths than the cryptography and set a limit to the true strength of the individual binding and hence the non-repudiation.

5.15 - How do we know when the system is becoming less secure?

Biometric systems may be initially adequately secure, but become less so with passing time. This could be because critical security parameters such as threshold settings become maladjusted, or sloppy enrolment procedures lead to poor enrolment quality. Some biometric systems are self-adaptive which means that the templates are updated each time a user accesses the system. This feature is intended to maintain the system performance (essentially to stop the false rejection rate increasing) if the users' biometric characteristics change over time. Such updating may result in the reference templates becoming weaker (easier for an impostor to attack) without supervisors being aware of anything untoward. The problem may be exacerbated if coupled with sloppy user behavior which results in poor quality images that translate into weaker templates.

5.16 - Does publicizing countermeasures make the systems less secure?

If details of countermeasures employed in biometric systems are publicized, it may help attackers to avoid or defeat them. Similarly, if attackers know what countermeasures are not employed, this will help them identify potential weaknesses in the system, and direct attacks towards those weak areas. The counter-argument is that public exposure of countermeasures and vulnerabilities will lead to a more mature and responsible attitude from the biometrics community and promote the development of more secure systems in the future. Generally, achieving security through obscurity is not seen as a viable policy as it depends on the assumed difficulty of analysis which is a hostage to fortune. For example the design of a "secure" mechanism may fall into the hands of an attacker and, if the underlying security is not adequate, compromise will result. Certainly in the traditional area of cryptography, the philosophy that is normally adopted is to assume that an opponent will have knowledge of the design of the cryptographic algorithm, but that knowledge should not compromise the cryptographic security. That is not to say that obscurity cannot provide any protection, rather that the protection is invariably unpredictable and may be short-lived. If we wish to make biometric devices and applications secure it is necessary to understand the threats and put in place effective countermeasures, technical and procedural. A parallel may be drawn with the field of IT vulnerabilities where the world has had time to come to terms with the idea and not seek to suppress knowledge. Rather, the approach is to report problems to the developers so that they can be fixed and patches issued. The balance between (excessive) publicity and suppression has been struck, founded on pragmatic principles based on experience. If and when biometrics are widely deployed, a similar approach can be expected to be adopted.

5.17 - Could I accidentally give my biometric 'signature'?

Users may be concerned that their biometric features could be captured without their consent or even knowledge and that they might thereby unintentionally unlock a door, or authorize a payment. If true, this could have serious financial or safety consequences, however it is rather unlikely because, in any real application, the issue would be addressed if applicable. Such considerations could limit the type of technology used in an application or impose requirements for clear explicit consent where the biometric alone is not deemed sufficient to provide consent. Non-biometric systems generally require an explicit user action. However, there are exceptions such as the use of contact-less (vicinity or proximity) smart cards or RFID tokens, which may be read as a user walks past a sensor. Such cards cannot be used as a method for giving authorization.

5.18 - Can my biometric be collected covertly?

Users may have concerns about being identified or tracked by covert applications (both legal and illegal). Users may feel they have a right to know when their biometrics are being collected and have a right to opt-out of biometric data collection. If biometrics can be collected covertly, they have no way to know whether such rights are being upheld. Examples are surveillance applications which are checking against a "watch list", looking for known terrorists or criminals, or something more innocuous like a commercial application looking for – say – favored customers in a shop. Some biometrics can be easily used 'covertly'. For example face recognition, speaker verification, and gait recognition can work from a distance. There is no obvious way of knowing whether a CCTV camera is biometrically enabled. Even close-up and contact biometrics could be used covertly – e.g. recognition of latent fingerprints, covert fingerprint sensor in doorknob, or iris recognition through a 1-way mirror.
Non biometric identifiers cannot be so easily covertly collected in most cases (but note the example of the contact-less or RFID cards). However cards can be copied and passwords divulged, unknown to the authorized user, with similar consequences.

5.19 - Can my biometric be stolen?

Can the biometric template or biometric feature vector be stolen, and if so what are the consequences? If biometric template data are stolen, either:

- Directly, from the stored reference templates.
- By capturing the data in transit within the system.
- On a communication path between the biometric capture device and the rest of the system.

then the template data could be reused by an impostor to recreate the identity of an authorized user without the user being present. This would undermine the authentication integrity and grant the impostor illegal access to the assets protected by the biometric authentication. If the stolen template includes associated data, then the associated data could be used separately and independently of the biometric data. Any user credentials or alternative authentication data (e.g. password) might be used to compromise the system or the user without exploiting the biometric data. The degree of compromise would depend on the data and the protective measures in place to prevent exploitation of captured data. If successful, this would be an example of identity theft (see separate concern), and all the ramifications for identity theft would follow. An additional threat may result if a captured biometric template can be reverse engineered. The biometric "image" thus produced might be used to construct an artefact or to discover (chance) zero-effort false matches in the criminal fraternity. This threat could be exploited more easily if the system stores biometric images which can be recovered to generate a ready supply of targets for such attacks.

6. References:

1. National Science and Technology Council. "*Speaker Recognition*"
2. Saurav Bhattacharyya and T. Srikanthan. Centre for High Performance Embedded Systems (CHiPES), "*Voice Biometrics, Emerging Trends & Challenges for Deployment*"
3. National Science and Technology Council. "*Dynamic Signature*"
4. National Science and Technology Council. "*Palm Print Recognition*"
5. Adams Konga, David Zhanga, Mohamed Kamelb. "*Palmprint identification using feature-level fusion*"
6. Jarmo Ilonen. "*Keystroke dynamics*"
7. Anil K. Jain. "*Biometric Authentication based on Keystroke Dynamics Authentication based on Keystroke Dynamics*"
8. John Daugman, PhD, OBE. "*How Iris Recognition Works*"
9. National Science and Technology Council. "*Hand Geometry*"
10. Yau Wei Yun. "*The '123' of Biometric Technology*"
11. Anil K. Jain, Arun Ross and Salil Prabhakar. "*An Introduction to Biometric Recognition*"
12. Biometrics Working Group (BWG). "*Biometric Security Concerns*"
13. D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar. "*Handbook of Fingerprint Recognition*"
14. Sriram Kalyanaraman. "*Biometric Authentication Systems*"
15. Zhanna Korotkaya. "*Biometric Person Authentication: Odor*"
16. Lily Lee. "*Gait Analysis for Recognition and Classification*"
17. Mark Ruane Dawson. "*Gait Recognition*"
18. Yi Chen, Sarat Dass, Arun Ross, and Anil Jain. "*Fingerprint Deformation Models Using Minutiae Locations and Orientations*"
19. National Science and Technology Council. "*Fingerprint Recognition*"
20. Arun Rossa, Jidnya Shaha and Anil K. Jainb. "*Towards Reconstructing Fingerprints From Minutiae Points*"
21. Ankie van der Zanden. "*Matching Fingerprints*"
22. Stephen A. Mascaro, H. Harry Asada. "*The common patterns of blood perfusion in the fingernail bed subject to fingertip touch force and finger posture*"
23. M. Turk and A. Pentland, "*Eigenfaces for Recognition*"
24. National Science and Technology Council. "*Face Recognition*"
25. D. Swets and J. Weng, "*Using Discriminant Eigenfeatuers for Image Retrieval*"
26. Laurenz Wiskott, Jean-Marc Fellous, Norbert Krüger, Christoph von der Malsburg. "*Face Recognition by Elastic Bunch Graph Matching*"
27. Hanna-Kaisa Lammi. "*Ear Biometrics*"