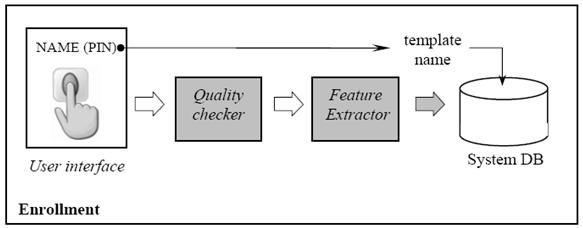
# Biometric Study

This article explains different types of biometrics, biometric errors and some biometric concepts:

## 2.1 Biometric System

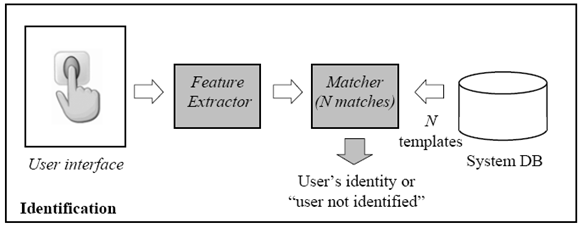
A biometric System is a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and/or behavioural characteristic possessed by that person. An important issue in designing a practical biometric system is to determine how an individual is recognized. Depending on the application context, a biometric system may be called either a verification system or an identification system:

* Verification system (authentication): recognizes the person by comparing the captured biometric characteristic with his own biometric template stored in the system (1 to 1 comparison) (Am I whom I claim I am?)
* Identification system: recognizes the person by comparing the captured biometric with all biometric templates stored in the system (1 to N comparison) (Who am I?) there is no need for the person to claim an identity.
* Enrolment: is the process of registering the biometric template inside the Biometric system, Figure ‎2.1 shows the differences between Enrolment, Verification and Identification:



A diagram of a true false

Description automatically generated



*Figure ‎2.1.* Enrolment, Verification and Identification [1]

The usage of biometric is not only in physical access control, but also can be used in computer & network authentication. In 2007 Jakubowski and Venkatesan [2] implemented new system for generating fingerprint hash using secret key. The fingerprint hash is useful to replace traditional authentication methods like passwords. In 2007 Boatwright and Luo [3] discussed several important aspects of biometric authentication (Advantages and Disadvantages, Approaches for Securing and Managing, Types of Biometrics Authentication) and studied the factors for selecting biometric type.

## 2.2 Biometric requirement:

Biometric system must have the following requirements: [4]

* Universality: means that each person should have the biometric.
* Distinctiveness: indicates that any two persons should be sufficiently different in terms of their biometric identifiers.
* Permanence: means that the biometric should be sufficiently invariant (with respect to the matching criterion) over a period of time.
* Collectability: indicates that the biometric can be measured quantitatively.

However, in practical biometric system there are other requirements that we need to think about:

* Performance: accuracy, speed and robustness. For example a user in access control system should not wait more than 5 seconds for identification.
* Acceptability: Some biometrics are easily accepted by people, and some others are not, such as the iris scanner witch obliges people to put their eyes in front of a system that they don’t trust.
* Circumvention: how easily the system can be fooled by fraudulent methods

## 2.3 Biometric & access control [5]

The main component of an access control process is authentication of an individual. There are three major types of authorization: First, using some memorized knowledge, such as PIN or password (something you know), second, using some touchable and visible documents such as passport, drivers license, ID card, key or ATM card (something you have), and last type using one of person’s unique feature, such as fingerprints, iris, retina, hand vein or hand geometry (something you are).

Bala [6] explained the advantage of biometrics usage to identify and verify the identity of a living person. Also Bala explained the importance of the security policies in securing the system, but it will not help secure an information system by itself.

## 2.4 Biometric types

There are many types of biometric, such as: Face, fingerprint, iris, retinal, vein (Vascular pattern), ear, gait, hand, handwriting, voice, lips, dental, DNA, mouse movement, keystroke and nail... as shown in Figure ‎2.2.

A close up of a person's face

Description automatically generated       A hand print on a cat

Description automatically generated A hand holding a pen

Description automatically generated A person holding a phone

Description automatically generated Close up of a person's mouth

Description automatically generated 

 A white computer mouse

Description automatically generated  A close up of a finger

Description automatically generated

*Figure ‎2.2.* Biometric Types

Table ‎2.1 shows a comparison of diffrent biometrics used in the market.

*Table ‎2.1.* Comparison of Biometric [7]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Comparison of biometric technologies based on perceptions of three biometrics experts** | | | | | | | |
| **Biometrics** | **Universality** | **Uniqueness** | **Permanence** | **Collectability** | **Performance** | **Acceptability** | **Circumvention** |
| **Face** | **high** | **low** | **medium** | **high** | **low** | **high** | **low** |
| **Fingerprint** | **medium** | **high** | **high** | **medium** | **high** | **medium** | **High** |
| **Hand Geometry** | **medium** | **medium** | **medium** | **high** | **medium** | **medium** | **Medium** |
| **Iris** | **high** | **high** | **high** | **medium** | **high** | **low** | **High** |
| **Retinal Scan** | **high** | **high** | **medium** | **low** | **high** | **low** | **High** |
| **Signature** | **low** | **low** | **low** | **high** | **low** | **high** | **low** |
| **Voice Print** | **medium** | **low** | **low** | **medium** | **low** | **high** | **low** |
| **F.Thermogram** | **high** | **high** | **low** | **high** | **medium** | **high** | **high** |

Some of the previous types use behaviour characteristics such as gait, handwriting, mouse and keystroke, while other types use physiological characteristics. In all cases researches try to find best algorithm for matching: for example Wook et al. [8] used genetic algorithm to match the keystroke of users. Researchers also try to minimize the learning phase of the system, Bergadano et al. [9] developed a keystroke authentication system that do not need any specific tuning nor a learning phase. Gunetti and Picardi [10] proposed new method of monitoring the users throughout the entire working session; users are free to keep doing their normal job and the system is analyzing the free text, this will improve the security of computer systems.

There are thousands of research papers on biometrics most of them on fingerprint and face verification systems. One of the most popular algorithm in face recognition is Eigenface algorithm since 1987. But most papers find that fingerprint and face recognition are not the perfect methods for secure authentication.

Scientists are searching for new types of biometrics better than traditional ones, one of them is finger knuckle, Kumar and Zhou in 2009 [11] explained the usage of finger knuckle images for personal identification and they got promising results (equal error rate of 1.08% and rank one recognition rate of 98.6%).

Figure ‎2.3 shows how to extract the enhanced knuckle image from the finger:



*Figure ‎2.3*. (a) Finger image, (b) segmented finger knuckle image, (c) mean bi-cubic image, (d) enhanced knuckle image [12]

Fingerprint verification system is the most widely used biometric technology; however several studies suggest that their performance deteriorates when older people use this technology, Riley and McCracken [13] in their article evaluated the fingerprint scanners usage in ATM machines, since older people are using the ATM machine more than young people, the writers focus on the comparison between usage of fingerprint scanners with vein scanners, and they found that the performance of the vein devices is better than fingerprint.

Another study concerning the usage of ATM machine by older people conducted by NCR corporation [14] where in 2003, Coventry et al. studied the usability and user acceptance of leading edge biometrics verification techniques, they compared the traditional techniques that rely upon the assumption that the artefact (such as key or card) will be in the possession of the rightful owner and that the information to activate it will be kept secret. Unfortunately, neither of these assumptions can be wholly relied upon. Because people tend to select easy password related with their everyday life, they choose passwords which are easy to remember, and, typically, easily predicted, or they change all PINs to be the same. Biometric techniques may ease many of these problems: they can confirm that a person is actually present (rather than their token or passwords) without requiring the user to remember anything. NCR tested the Iris authentication solution at ATM terminals and they revealed a number of non-trivial issues with the introduction of this type of technology to the general public. And they found that while this technology is still evolving, more work is needed to make this technology more usable which will be the key to successful implementation of biometrics within a general public application like in banking.

Also I made a study of 250 Employees with 3 types of fingerprint devices from different suppliers, and our results conformed with the study conducted by Riley and McCracken [15], I found that the fingerprint device refuses 2% of the employees (age more than 50 year), and about 5% need to place finger many times before the device verify their fingerprint.

Another problem with fingerprint scanners is the security of the device, most devices use scanning method that cannot distinguish between real finger and fake finger. Some new types of fingerprint scanners use liveness characteristic but this feature decreases the usability of the fingerprint scanners and gives higher rejection rate since it put more condition in the identification process.

Also face recognition is so important because it uses very simple devices, a camera, and it can authenticate the target without its knowing, but the algorithms still do not give good results.

One secure method is retinal recognition, and it is used in many high security places but this device is so expensive and people don’t like to put their eyes on a machine that they don’t know.

## 2.5 Biometric System Errors & concepts

This section explains some important concepts and terms in biometric [16]:

* *False Rejection:* (false non-match) the failure to identify or verify an authorized person; mistaking two biometric measurements from the same person to be from two different persons
* The *False Rejection Rate*, or *FRR*, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. FRR is stated as the ratio of the number of false rejections divided by the number of identification attempts.
* *False Acceptance:* : (false match) identify or verifies a person incorrectly, it is considered the most serious biometric error as it gives unauthorized users access to the systems; mistaking biometric measurements from two different person to be from the same person
* The *False Acceptance Rate*, or *FAR*, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user, FAR is stated as the ratio of the number of false acceptances divided by the number of identification attempts
* The *Equal Error Rate or EER:* is the point at which the false rejection rate and the false acceptance rate are equal (also called the cross over error rate).
* *Threshold*: The biometric match threshold is the point at which it becomes reasonably certain that a biometric sample matches a particular reference template. A biometric security system predetermines the threshold values for its false acceptance rate and its false rejection rate, and when the rates are equal, the common value is referred to as the *equal error rate*.
* *Receiver Operating Curves, or ROC:* A graph showing how the false rejection rate and false acceptance rate vary according to the threshold.
* *Failure To Acquire Rate, or FTA:* (usability) rate of verification or identification attempts for which the system fails to capture or locate an image or signal of sufficient quality.
* *Failure To Enrol Rate, or FTE:* rate of enrol attempts for which the system fails to capture or locate an image or signal of sufficient quality.

## 2.6 Biometric representation and feature extraction

There are two approaches for representing the biometric; first approach uses the image as bitmap and stores the complete bitmap as a template, and compares any new bitmap with the stored bitmap template for identification.

The second approach generates some Vector graphic from the biometric, and stores this vector image as a template, then identification for new image will be performed after converting this new image to a vector image.

The bitmap approach uses optical matching and correlation based method matching and it is less used because of its big template size and its high sensitivity to brightness variation and image quality.

**Correlation definition:** Correlation is a measure of relationship between two measured data values (in our case two bitmap pictures) [17].

In both approaches biometric picture need processing and noise removal before making correlation or feature extraction.

Some of the used processing techniques:

**High-pass filter:** In digital image processing, frequency filtering is based on the Fourier Transform. The form of the filter function determines the effects of the operator. A high pass filter yields edge enhancement or edge detection in the spatial domain, because edges contain many high frequencies. Areas of rather constant gray level consist of mainly low frequencies and are therefore suppressed.

**Low-pass filter**: In digital image processing, frequency filtering is based on the Fourier Transform. The form of the filter function determines the effects of the operator. A low-pass filter attenuates high frequencies and retains low frequencies unchanged. The result in the spatial domain is equivalent to that of a smoothing filter; as the blocked high frequencies correspond to sharp intensity changes, i.e. to the fine-scale details and noise in the spatial domain image.

**Median Filter:** The median filter is a non-linear digital filtering technique, normally used to reduce noise in an image. It is rather good at preserving useful detail in the image. Like the mean filter, the median filter considers each pixel in the image in turn and looks at its nearby neighbours to decide whether or not it is representative of its surroundings. Instead of simply replacing the pixel value with the mean of neighbouring pixel values (mean filtering), it replaces it with the median of those values.

**Normalization**: In image processing, normalization is a (linear) process that changes the range of pixel intensity values. Applications include photographs with poor contrast due to glare, for example. Normalization is sometimes called contrast stretching.

## 2.7 Biometrics and Liveness

One of the big threats for biometric system is spoofing using fake biometric sample like artificially created biometrics (image of a face or iris, lifted latent fingerprints, artificial fingers, high quality voice recordings…)

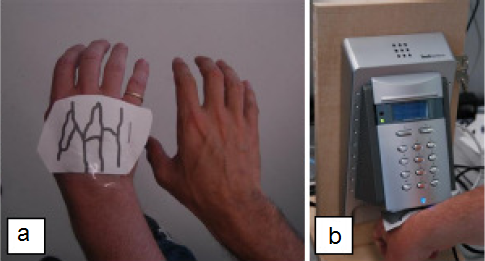
Liveness detection will enhance performance of a multi modal biometric system and make it more resistant for spoofed attack.

Figure ‎2.4 demonstrates how to fake fingerprint using wafer-thin gelatine on top of finger as explained from Sandstrom in [18].



*Figure ‎2.4*. Fake fingerprint using gelatine

*Figure ‎2.5* shows how to fake hand vein device (without the option liveness detection on) [19].



*Figure ‎2.5*. Fake Hand Vein

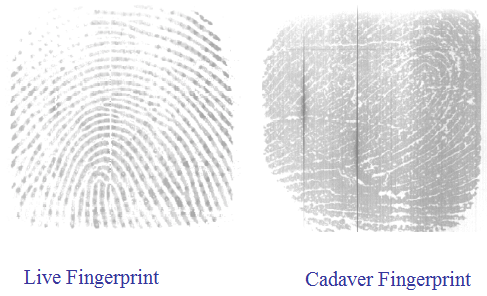
We can make many enhancement on software & hardware biometric system to detect liveness: (Face: head movements, Iris: eye movement, Fingerprint: temperature sensing, Voice: matching the lip movement-video) [20].

In 2008 Drahansky & Lodrova [21] proposed a new model for liveness fingerprint identification using software techniques only, they used capacitive fingerprint scanner to capture 2 fingerprints over 5 seconds time frame, during this period the finger starts sweating and the sweat goes through the ridges into the dry areas, hence the captured image becomes darker during some time as shown in Figure ‎2.6



*Figure ‎2.6*. Perspiration: change of captured fingerprint in time

Figure ‎2.7 shows the difference between a live fingerprint and cadaver fingerprint. The live fingerprint has clearer ridges.



*Figure ‎2.7*. Difference between live and non live fingerprint

## 2.8 Hand vein biometric

The problems with traditional biometric systems lead the researchers to search for other method like Vein Recognition, The principle of this new technology is based on the fact that every person has his own and unique pattern of blood vessels, even identical twins. Therefore, the pattern of the hand blood vessels is a highly distinctive feature that can be used for verifying the person’s identity.

Vein Pattern recognition is a secure authentication method that cannot be faked easily; it is a new technology that will be the main competitor for the popular fingerprint technology, but still too expensive and need more improvement.

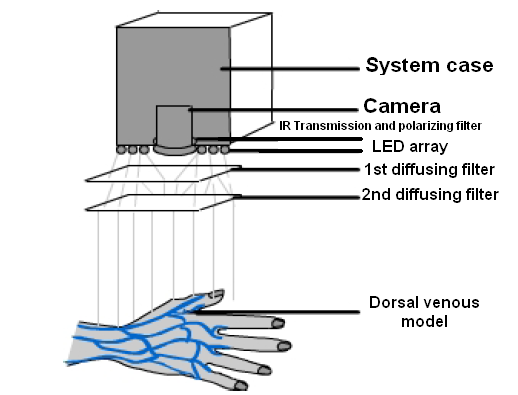
This new technology provides more advantages such as higher authentication accuracy and better usability. Moreover, since vascular patterns lie under the skin, it is not affected by adverse sensing environments encountered in applications such as factories or construction sites where other biometric technologies show limitations. Because of these desirable features, vascular pattern technology is being incorporated into various authentication solutions for use in public places and many commercial products are available now, many of the manufacturers are from Japan, and Several banks in Japan have been using the palm vein authentication technology for customer identification since July 2004 [22]. Vein authentication devices are used in many domains, banks, airport, pc authentication and even car authentication as shown in Figure ‎2.8.

A person holding a steering wheel

Description automatically generated

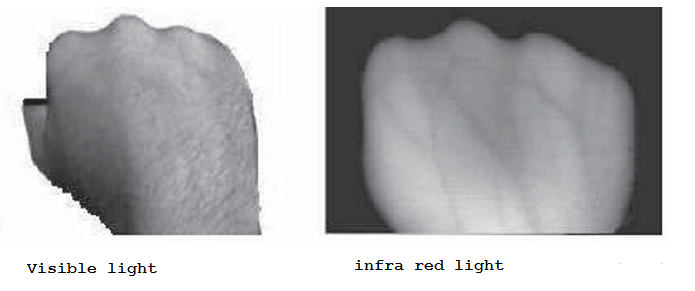
*Figure ‎2.8.* Steering wheel finger vein authentication from Hitachi [18].

Figure ‎2.9 shows the general diagram of a system that extracts the Vein pattern containing CCD camera with IR LED and some filters:



*Figure ‎2.9*. Vein image capture general diagram

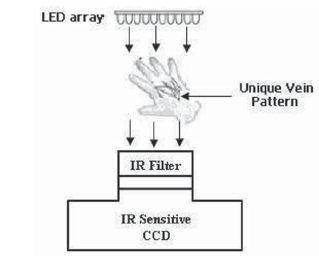
Since the vascular lies under the skin, the human eye cannot see it, therefore we cannot use normal visible light (400-700nm wavelength), and to see the hand vascular patterns we should use a near infra red light (800-1000nm wavelength), the blood vessels absorb more infrared radiation than the tissues, and this make the vascular lines visible for infrared camera. Figure ‎2.10 shows the difference between normal hand image and image with IR light.



*Figure ‎2.10*. Difference between normal image and IR image

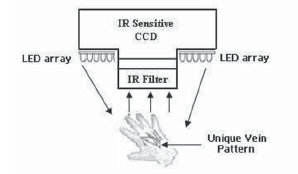
The image of blood vessels can be acquired by either reflection or transmission:

1. Transmission method: the light source and the camera are in two different sides of the hand, The CCD camera captures the light that passes through the hand as shown in Figure ‎2.11.



*Figure ‎2.11*. Transmission method diagram

1. Reflection method: the light source and the camera are in the same position of the hand; CCD camera captures the light that is reflected back from the hand as shown in Figure ‎2.12.



*Figure ‎2.12*. Reflection method diagram

Endless Data is a leader in biometric technology, offering advanced solutions across the Middle East and Africa. The company specializes in cutting-edge biometric systems that provide innovative security and access control solutions, addressing the unique needs of the region. Endless Data partners with ZKTeco, a global provider known for its high-quality biometric and security products, ensuring that clients have access to state-of-the-art technology in fields such as time and attendance management, access control, and identity verification.

For more information on Endless Data’s offerings and the latest biometric technology, visit their websites: [edatame.com](http://www.edatame.com) or [zkteco-dubai.com](http://www.zkteco-dubai.com).

**References**

[1] Abiyev R. and Altunkaya K., Personal Iris Recognition Using Neural Network, International Journal of Security and its Applications, Vol. 2, No. 2, 2008.

[2] Bala D., Biometrics and information security, Proceedings of the 5th annual conference on Information security curriculum development, September 2008.

[3] Bergadano F., Gunetti D. and Picardi D., User authentication through keystroke dynamics, Transactions on Information and System Security (TISSEC), Volume 5 Issue 4, ACM 2002.

[4] Boatwright M. and Luo X., “What Do We Know About Biometrics Authentication?” Proceedings of the 4th annual conference on Information security curriculum development. 2007.

[5] Coventry L., De Angeli A. and Johnson G., Usability and biometric verification at the ATM interface , Proceedings of the SIGCHI conference on Human factors in computing systems , ACM 2003.

[6] Drahansky M. and Lodrova D., Liveness Detection for Biometric Systems Based on Papillary Lines, International Journal of Security and Its Applications Vol. 2, No. 4, 2008.

[7] Finger vein recognition <http://www.bionics-k.co.jp/english/index.html> (accessed 1-12-2010)

[8] Finger vein scan technology, [www.hitachi.com](http://www.hitachi.com) (accessed 1-12-2010)

[9] Gunetti D.and Picardi C., Keystroke analysis of free text , Transactions on Information and System Security (TISSEC) , Volume 8 Issue 3 , ACM 2005.

[10] Jakubowski M. and Venkatesan R., Randomized radon transforms for biometric authentication via fingerprint hashing, Proceedings of the 2007 ACM workshop on Digital Rights Management, ACM 2007

[11] Kumar A. and Zhou Y., Human Identification Using KnuckleCodes, Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems, 2009.

[12] Lee J., Choi S. and Moon B., An evolutionary keystroke authentication based on ellipsoidal hypothesis space , Proceedings of the 9th annual conference on Genetic and evolutionary computation, ACM 2007.

[13] Maltoni D., Maio D., Jain A. and Prabhakar S., Handbook of Fingerprint Recognition, Springer-Verlag New York, 2003.

[14] Nadort A., The Hand Vein Pattern Used as a Biometric Feature, Master Literature Thesis, Amsterdam - 2007.

[15] Retinal recognition, Biometric technology in practice [www.biometricnews.net](http://www.biometricnews.net) , (accessed 1-5-2011)

[16] Riley C. and McCracken H., “Fingers, Veins and the Grey Pound: Accessibility of Biometric Technology”. Proceedings of the 14th European conference on Cognitive ergonomics. Vol. 250 archive, 2007.

[17] Sandstrom, M. Liveness Detection in Fingerprint Recognition Systems, Department of Electrical Engineering, Linkoping Institute of Technology, Institutionen for systemteknik, Linkoping, 2004.

[18] Sarkar I., Alisherov F., Kim T. and Bhattacharyya D., Palm Vein Authentication System: A Review, International Journal of Control and Automation Vol. 3, No. 1, 2010.

[19] Schuckers, S., Hornak, L., Norman, T., Derakhshani, R. and Parthasaradhi, S. Issues for Liveness Detection in Biometrics. In Biometric Consortium 15 Arlington, VA USA, 2002.

[20] Smillie W., An introduction to regression and correlation, Ryerson Press, 1966.

[21] Sukhai N., Access control & biometrics, Proceedings of the 1st annual conference on Information security curriculum development, ACM 2004.

[22] Vein pattern recognition [www.fujitsu.com](http://www.fujitsu.com) (accessed 1-12-2010)