Personal Identification Through Biometric Technology

Hazem M. El-Bakry
Faculty of Computer Science & Information Systems,
Mansoura University, EGYPT
E-mail: helbakry20@yahoo.com

Nikos Mastorakis
Technical University of Sofia,
BULGARIA

Abstract:
With the evolution of information technology, our society is becoming more and more electronically connected. Daily transactions between individuals or between individuals and various organizations are conducted increasingly through highly interconnected electronic devices. The capability of automatically establishing the identity of individuals is thus essential to the reliability of these transactions. For many reasons, new techniques must be emitted in order to solve the problem of automatic personal identification. First, the current level of security does not match the specifications defined for the application. Second, fraud in the current application is too high and uncontrollable. Third, current verification methods are expensive and unreliable. Traditional personal identification approaches which use "something that you know" such as Personal Identification Number (PIN), or something that you have such as an Identification tag (ID card, like a padge for example) are not sufficiently reliable to satisfy the security requirements of electronic transactions because they lack the capability to differentiate between a genuine individual and an imposture who fraudulently acquires the access privilege. Biometric approaches of identification are enjoying a renewed interest. They refer to automatic recognition of individuals based on a feature vectors derived from their physiological like Face, Fingerprint and/or behavioral characteristic such as Signature. Biometric recognition systems should provide reliable personal recognition schemes to either confirm or determine the identity of an individual. By using biometrics a person could be identified based on "who she/he is" rather then "what she/he has" (card, token, key) or "what she/he knows" (password, PIN). In this paper, the study presented in [77] is extended. A brief overview of biometric methods, both unimodal and multimodal, as well as their advantages and disadvantages are presented. Furthermore, combined techniques for authentication are introduced. In addition, more attention for palm vein recognition is given. Vein pattern biometrics presents many advantages over outdated biometric methods. Vein-pattern biometric technologies require little physical contact. Furthermore, they are unique to each user In addition, they are fast and easy to use. Moreover, this pattern will not vary over the course of a person's lifetime

Keywords: Personal Identification, Biometrics, Pattern Recognition

1. Introduction

The term biometric comes from the Greek words bios (life) and metrikos (measure). It is well known that humans intuitively use some body characteristics such as face, gait or voice to recognize each other. Since, today, a wide variety of applications require reliable verification schemes to confirm the identity of an individual, recognizing humans based on their body characteristics became more and more interesting in emerging technology applications [1]. Traditionally, passwords and ID cards have been used to restrict access to secure systems but these methods can easily be breached and are unreliable. Biometrics can not be borrowed, stolen, or forgotten, and forging one is practically impossible [1].

2. Biometrics

There are several biometric technologies in use today with a few more technologies being investigated in research laboratories worldwide. Nevertheless, all the technologies share a common process flow as follows [1,3]:

2.1: Some of the current and potential Biometrics are [2]:

- Voice
- Fingerprints
- Face
- Iris
- Ear
- vein
- DNA
- Odor
- Infrared facial thermography
- Gait
- Keystroke dynamics
- Signature
- Retinal scan
- Hand & finger geometry
- Subcutaneous blood vessel Imaging

2.2: These biometrics should be characterized by [2]

Universality, Uniqueness, Stability, Collectability, Performance, Acceptability, Forge resistance

2.3: Biometrics could be categorized as either physical or behavioral

2.3.1: Physical biometrics [3,4]:

1. Fingerprint—Analyzing fingertip patterns

2. Facial recognition/face location—Measuring facial characteristics
3. Hand geometry—Measuring the shape of the hand
4. Iris scan—Analyzing features of colored ring of the eye
5. Retinal scan—Analyzing blood vessels in the eye
6. Vascular patterns—Analyzing vein patterns
7. DNA—Analyzing genetic makeup
8. Biometric data watermarking (which is really a method rather than a physical attribute) is used to store/hide biometric information.

2.3.2: Behavioral biometrics [3]:

1. Speaker/voice recognition—Analyzing vocal behavior
2. Signature/handwriting—Analyzing signature dynamics
3. Keystroke/patterning—Measuring the time spacing of typed words

3: Biometric Systems [4]

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses. The common process flow of biometrics is shown in Fig. 1. A particular biometric system should be able to:

1. Achieve acceptable identification accuracy and speed with a reasonable resource requirements.
2. Not be harmful to the subjects and be accepted by the intended population
3. Be sufficiently robust to various fraudulent methods.

This method of identification is preferred over current methods involving passwords and PIN numbers for various reasons:

1- The person to be identified is required to be physically present at the point-of-identification.

2- Identification based on biometric techniques obviates the need to remember a password or carry a token.

3- Biometric techniques are not easily countrified.

Thus biometric approaches of identification are enjoying a renewed interest.

3.1: A simple biometric system consists of four basic components:[16]

1) Sensor module which acquires the biometric data; Web cam, Digitizing Table, Scanner.
2) Feature extraction module where the acquired data is processed to extract feature vectors; Projection [offline], DCT on Coordinates [online, offline]
3) Matching module where feature vectors are compared against those in the template ;(Neural Networks, Algorithm)
4) Decision-making module in which the user's identity is established or a claimed identity is accepted or rejected. (Final results)

4. Overview of commonly used biometrics

Since there are number of biometric methods in use (some commercial, some "not yet"), a brief overview of various biometric characteristics will be given, starting with newer technologies and then progressing to older ones.

4.1: Signature:[12]

Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. Collecting samples for this biometric includes subject cooperation and requires the writing instrument. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of a subject. In addition to the general shape of the signed name, a signature recognition system can also measure pressure and velocity of the point of the stylus across the sensor pad.

4.1.1: Signature recogntion:

Biometric signature recognition systems measures and analyzes the physical activity of signing, such as the stroke order, the pressure applied and the speed. Some systems may also compare visual images of signatures, i.e. how it is signed rather than visual, i.e. the image of the signature. Processing of signature images is shown in Fig. 2, while offline signature recognition system is shown in Fig. 3.

4.1.2: Benefits of signature biometric systems

1. While it is easy to copy the image of signature, it is extremely difficult to mimic the behavior of signing.
2. Low False Acceptance Rates (FAR)
3. People are used to sign documents, so signature recognition systems are not perceived to be invasive

4.1.3: Weaknesses of signature biometric systems

1. People may not always sign in a consistent manner

4.2: Fingerprint [7]

Finger print is the oldest method of identity authentication and has been used since 1896 for criminal identification. The fingertips have

corrugated skin with line like ridges flowing from one side of the finger to another. The flow of the ridges is non-continuous and forms a pattern. The discontinuity in the ridge flow gives rise to feature points, called minutiae, while the pattern of flow give rise to classification pattern such as arches, whorls and loops. These are the basis of fingerprint recognition. In forensic application, the fingerprints of criminal suspects are acquired (traditionally using the ink-and-roll procedure) and stored centrally. Identity search is then conducted using an Automated Fingerprint Identification System (AFIS) to narrow the search to one or a few prime suspects when a crime occurs. For civil applications, the fingerprint is not stored, but acquired live. The template which represents the fingerprint is stored rather than the image. There are a few variants of image capture technology available for such commercially oriented fingerprint sensor, including optical, silicon, ultrasound, thermal and hybrid [7]. There are two main technical approaches for fingerprint recognition: minutia matching and pattern matching. The former approach locates all the minutiae in the fingerprint consisting mainly ridge ending (where the ridge ends) and bifurcation (where the ridge branches into two). Other possible minutiae include dot (very short ridge), island (two nearby bifurcations), crossover (two ridges crossing each other) and pore. From the geometric information, type, direction and relationship of the minutiae, comparisons can be made in order to establish whether the two minutia template matched or not. The latter approach utilizes the region surrounding a minutiae or other distinct mark and extrapolates data from the series of ridges in this region. For matching, the same area need to be found and compared and methods to handle deformation in the pattern is devised. Typically, the template size of the pattern matching approach is 2-3 times larger than in minutia approach. It is almost impossible to recreate the fingerprint image from the minutia based template but this cannot be said for the pattern matching approach. In addition, all the AFIS systems used in forensic applications is minutia based and is an accepted approach in a court of law. Thus majority of the fingerprint recognition system uses the minutia approach [7]. In general, fingerprint recognition can achieve good accuracy sufficient for both verification and identification. It is low cost and compact and is getting popular as consumer products. However, not everyone has fingerprints that can be recognized. The sensor is also not able to capture acceptable quality fingerprint images for people with very wet and very dry skin. In addition, the sensor needs to be maintained properly in order to get consistent performance. The Spring 2002 international developer survey conducted by Evans Data recently has concluded that fingerprints have the most potential in terms of user authentication [7]. The fingerprint image is shown in Fig. 4.

4.2.1: Fingerprint Scanner [17]

The scanner shown Fig. 5 is attached to a computer which uses algorithms to look for general patterns—whorls, arches, loop—as well as fine details known as minutiae and record these characteristics as encoded data.

4.3: Hand geometry [5]

This approach uses the geometric shape of the hand for authenticating a user's identity. Authentication of identity using hand geometry is an interesting problem. Individual hand features are not descriptive enough for identification. However, it is possible to devise a method by combining various individual features to attain robust verification. The hand image is obtained using a camera looking from the top when the user placed his or her hand at a specified surface. The hand can be aligned using pegs or reference marks. Two views are usually taken in a single image, the top view and the side view. The side view is usually taken by the top camera as well using a side mirror. From the hand image, the fingers are located and the length, width, thickness, curvatures and their relative geometry measured. The hand geometry template size can be very small. It has acceptable accuracy for verification but not sufficient for identification. The major advantage is that most people can use it and as such, the acceptance rate is good. However, the system is rather bulky and may have problems with aging and health condition such as arthritis.

4.3.1: Previous works:

1- A Hand Geometry-Based Verification System: [17]

This system explores the use of hand geometry as a measure of a person's identity. The system consists of an acquisition device that captures the top view and side view of a user's right hand as he places it on the flat surface of the device. A snapshot of the user's hand is taken for processing. A set of features have been identified that could be used to represent a person's hand. These features include the lengths and widths of the fingers at various locations. Hand and finger geometry are shown in Fig. 6.

2- Deformable Matching of Hand Shapes for Verification [17]

This system involves designing a mechanism that would align hand shapes prior to verifying a

person's identity. Such an approach would enhance the integrity of the feature set made available during the verification stage.

3- Web-Access using Biometrics [17]
This work involves securing a website using biometrics. Users are granted access to a set of files in a web-site after their identity has been verified using Biometrics - Hand Geometry in particular. We believe biometrics based web-access will add a new layer of security over existing web-security systems.

4.4: scanning systems:

4.4.1: Retina [11]

Retinal recognition creates an "eye signature" from the vascular configuration of the retina which is supposed to be a characteristic of each individual and each eye, respectively. Since it is protected in an eye itself, and since it is not easy to change or replicate the retinal vasculature, this is one of the most secure biometric. Image acquisition requires a person to look through a lens at an alignment target, therefore it implies cooperation of the subject. Also retinal scan can reveal some medical conditions and as such public acceptance is questionable. The retina image is shown in Fig. 7.

4.4.2: Iris [11]

The iris begins to form in the third month of gestation and the structures creating its pattern are largely complete by the eight month. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette. Iris scanning is less intrusive than retinal because the iris is easily visible from several meters away. Responses of the iris to changes in light can provide an important secondary verification that the iris presented belongs to a live subject. Irises of identical twins are different, which is another advantage. Newer systems have become more user-friendly and cost-effective. A careful balance of light, focus, resolution and contrast is necessary to extract a feature vector from localized image. While the iris seems to be consistent throughout adulthood, it varies somewhat up to adolescence.Iris recognition is very accurate with very low false acceptance rate (wrongly identifying the impostor as the genuine user) and can be applied to both verification and identification. The identification speed is also very fast and it is relatively easy to verify whether the iris is from a living subject. However, the cost of the system is somewhat high and not compact. It also suffers from poor lighting, reflection and possibly glasses and may not be suitable for people with cataract and young children. In addition, some imaging system will require the user to be motionless for a while. A sample segmented Iris with Iris Code (at Top Left Corner) and iris scanning device is shown in Fig. 8. A fast complete system for iris recognition was presented in [66-76].

4.5: Authentication systems:

4.5.1: Voice [15,16]

Voice authentication or speaker recognition uses a microphone to record the voice of a person. The recorded voice is digitized and then used for authentication. The speech can be acquired from the user enunciating a known text (text dependent) or speaking (text independent). In the former case, the text can be fixed or prompted by the system. The text can also be read discretely or the entire text read out continuously. The captured speech is then enhanced and unique features extracted to form a voice template. There are two types of templates: stochastic templates and model templates. Stochastic templates require probabilistic matching techniques such as the popular Hidden Markov Model and results in a measure of likelihood of the observation given the template. For model templates, the matching techniques used are deterministic. The observation is assumed to be similar to the model, albeit some distortion. Matching result is obtained by measuring the minimum error distance when the observation is aligned to the model. The matching techniques popularly used for model templates include Dynamic Time Warping algorithm, Vector Quantization and Nearest Neighbors algorithm. As voice is a common means of communication, and with an extensive telephone network, a microphone becomes rather common and as such the cost of voice authentication can be very low and compact. Furthermore, it is relatively easy to use. However, voice varies with age and there can be drastic change from childhood to adolescence. Also illness and emotion may affect the voice as well as room acoustics and environmental noise. Variation in microphones and channel mismatch (use of different type and quality of microphones) is also a major problem for the widespread use of this biometric technology. Matching algorithms used in voice recognition are similar to those used in face recognition.

4.6: Biometric facial recognition systems:

4.6: Face [16]

4.6.1: Principles of face biometrics

The dimensions, proportions and physical attributes of a person's face are unique.

4.6.2: How does face biometrics work

Biometric facial recognition systems will measure and analyze the overall structure, shape and proportions of the face: Distance between the eyes, nose, mouth, and jaw edges; upper outlines of the eye sockets, the sides of the mouth, the location of the nose and eyes, the area surrounding the cheekbones. At enrollment, several pictures are taken of the user's face, with slightly different angles and facial expressions, to allow for more accurate matching. For verification and identification, the user stands in front of the camera for a few seconds, and the scan is compared with the template previously recorded. To prevent an image / photo of the face or a mask from being used, face biometric systems will require the user to smile, blink, or nod their head. Also, facial thermography can be used to record the heat of the face (which won't be affected by a mask). The main facial recognition methods are: feature analysis, eigenfaces, neural network, and automatic face processing. Fast algorithm for real-time face detection were presented in [23-65]. Different methods for robust face recognition were presented in [33,34,50,53,58,59,60,62,64,65].

4.6.3: Benefits of face biometric systems [15]

Not intrusive, can be done from a distance, even without the user being aware of it (for instance when scanning the entrance to a bank or a high security area).

4.6.4: Weaknesses of face biometric systems [15]

1 - Face biometric systems are more suited for authentication than for identification purposes, as it is easy to change the proportion of one's face by wearing a mask, a nose extension, etc.

2- User perceptions / civil liberty: Most people are uncomfortable with having their picture taken.

4.6.5: Applications of face biometrics [15]

Access to restricted areas and buildings, banks, embassies, military sites, airports, law enforcement. Face recognition is generally accepted by the public, easy to use, a covert process, compact and the cost is rather low. The disadvantage is that the accuracy achievable it is only suitable for verification, but is still insufficient for identification. The performance will also be affected by variation in face due to aging, make-up, hair-style, glasses, pose and lighting condition in addition to not being able to separate twins.

4.6.6: 3D Face Recognition [14]

The performance of face recognition systems that use two-dimensional (2D) images is dependent on consistent conditions such as lighting, pose and facial expression. In a multi-view face recognition system is being developed, which utilizes three-dimensional (3D) information about the face, along with the facial texture, to make the system more robust to those variations. A procedure is presented for constructing a database of 3D face models and matching this database to 2.5D face scans which are captured from different views. 2.5D is a simplified 3D (x, y, z) surface representation that contains at most one depth value (z direction) for every point in the (x, y) plane. A robust similarity metric is defined for matching. Current experiments are conducted on a test bed of 100 3D models with 598 independent test scans.

4.7: Odor [3,4]

Each object spreads around an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. This would be done with an array of chemical sensors, each sensitive to a certain group of compounds. Deodorants and perfumes could lower the distinctiveness.

4.8: Ear [3,4]

It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. Matching the distance of salient points on the pinna from a landmark location of the ear is the suggested method of recognition in this case. This method is not believed to be very distinctive. Personal Identification through ear recognition is shown in Fig. 9.

4.9: Gait [3,4]

This is one of the newer technologies and is yet to be researched in more detail. Basically, gait is the peculiar way one walks and it is a complex spatio-temporal biometrics. It is not supposed to be very distinctive but can be used in some low-security applications. Gait is a behavioral biometric and may not remain the same over a long period of time, due to change in body weight or serious brain damage. Acquisition of gait is similar to acquiring a facial picture and may be an acceptable biometric. Since video-sequence is used to measure several different movements this method is computationally expensive.

4.10: Keystroke [3,4]

It is believed that each person types on a keyboard in a characteristic way. This is also not very distinctive but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one could expect to observe large variations in typical

typing patterns. Advantage of this method is that keystrokes of a person using a system could be monitored unobtrusively as that person is keying information. Another issue to think about here is privacy.

4.11 : DNA analysis [11]

Deoxyribonucleic acid (DNA) is probably the most reliable biometrics. It is in fact a one-dimensional code unique for each person. Exceptions are identical twins. The analysis of a sperm is shown in Fig. 10.

4.11.1: This method, however, has some drawbacks: [3]

1. Contamination and sensitivity, since it is easy to steal a piece of DNA from an individual and use it for an ulterior purpose,
2. No real-time application is possible because DNA matching requires complex chemical methods involving expert's skills,
3. Privacy issues since DNA sample taken from an individual is likely to show susceptibility of
4. a person to some diseases. All this limits the use of DNA matching to forensic applications.

Forensic scientists can use DNA located in blood, semen, skin, saliva or hair left at the scene of a crime to identify a possible suspect, a process called genetic fingerprinting or DNA profiling [11]. In DNA profiling the relative lengths of sections of repetitive DNA, such as short tandem repeats and minisatellites, are compared. DNA profiling was developed in 1984 by English geneticist Alec Jeffreys of the University of Leicester, and was first used to convict Colin Pitchfork in 1988 in the Enderby murders case in Leicestershire, England. Many jurisdictions require convicts of certain types of crimes to provide a sample of DNA for inclusion in a computerized database. This has helped investigators solve old cases where the perpetrator was unknown and only a DNA sample was obtained from the scene (particularly in rape cases between strangers).

5. Why Using Biometrics [16]

1. Convenience for users
2. Control for businesses
3. Inexpensive implementation
4. Price/Performance curves dropping
5. Saves money (i.e., no need for producing keys, etc.)
6. Accountability/Non-Repudiation
7. Improved identification (i.e., authentication, verification,
8. mpersonation)
9. Improved audit trail
10. Less administration (i.e., paperwork, cards, etc.)
11. More security ?

5.1: Biometrics Comparison Chart [19]

The comparison of different types of biometrics is shown in Fig. 14.

6. Understanding Hand Scanning [17]

This biometric approach uses the geometric form of the hand for confirming an individual's identity. Because human hands are not unique, specific features must be combined to assure dynamic verification. Some hand-scan devices measure just two fingers, others measure the entire hand. These features include characteristics such as finger curves, thickness and length; the height and width of the back of the hand; the distances between joints and overall bone structure. It should be noted that although the bone structure and joints of a hand are relatively constant traits, other influences such as swelling or injury can disguise the basic structure of the hand. This could result in false matching and non-false matching, however the amount of acceptable distinctive matches can be adjusted for the level of security needed.

To register in a hand-scan system a hand is placed on a reader's covered flat surface. This placement is positioned by five guides or pins that correctly situate the hand for the cameras. A succession of cameras captures 3-D pictures of the sides and back of the hand. The attainment of the hand-scan is a fast and simple process. The hand-scan device can process the 3-D images in 5 seconds or less and the hand verification usually takes less than 1 second. The image capturing and verification software and hardware can easily be integrated within standalone units. Hand-scan applications that include a large number of access points and users can be centrally administered, eliminating the need for individuals to register on each device. The images of hand veins are shown in Fig. 11. Palm vein authentication system (palm graph) and finger vein authentication system are shown in Fig. 12. The scan result for the palm veins of the human hand is shown in Fig. 13.

6.1 : Applications for Hand scanning:

Internationally, many airports use hand-scan devices to permit frequent international travelers to by-pass waiting lines for various immigration and customs systems. Employers use hand-scan for entry/exit, recording staff movement and time/attendance procedures. This can go long

way to eradicating the age old problem of buddy-clocking and other deceptive activities.

6.2: Why I use the hand scanning as the main feature for the identification process?

Hand-scanning can be easily combined with other biometrics such as fingerprint identification or signature identification. A system where fingerprints are used for infrequent identification and hand-scanning is used for frequent verification would create a two tiered structure. The hand-scan component used frequently allows identity verification or 1:1 (one to one) verification that ensures the user is who they claim they are. The fingerprint identification component used infrequently, confirms who the user is and accurately identifies the user in a 1:N (one to many) identification that is compared with numerous records.

6.3 : why I use the vein-recognition as the main hand-scanning feature for the identification process?

The need for effective, repeatable biometric technologies has increased during our war on terror and the recent plague of identity thefts. Vein pattern biometrics presents many advantages over outdated biometric methods. Vein-pattern biometric technologies require little physical contact, are unique to each user and are fast and easy to use, Furthermore, this pattern will not vary over the course of a person's lifetime.

6.4: How does palm vein biometrics work [21]

An individual's vein pattern image is captured by radiating his/her hand with near-infrared rays. The reflection method illuminates the palm using an infrared ray and captures the light given off by the region after diffusion through the palm. The deoxidized hemoglobin in the in the vein vessels absorbs the infrared ray, thereby reducing the reflection rate and causing the veins to appear as a black pattern. This vein pattern is then verified against a preregistered pattern to authenticate the individual.

As veins are internal in the body and have a wealth of differentiating features, attempts to forge an identity are extremely difficult, thereby enabling a high level of security. In addition, the sensor of the palm vein device can only recognize the pattern if the deoxidized hemoglobin is actively flowing within the individual's veins.

This sytem is not dangerous, a near infrared is a component of sunlight: there is no more exposure when scanning the hand than by walking outside in the sun.

6.5: Vein Pattern Advantages [19]

1. The human vascular structure is a unique & private feature of an individual.
2. Infra Red absorption patterns are easily compared via optical and DSP techniques.
3. Identical twins have different and distinct IR absorption patterns.
4. Uniqueness of vein patterns tested by Cambridge Consultants Ltd.
5. Veins provide large, robust, stable and hidden biometric features.
6. Vein patterns are not easily observed, damaged, obscured or changed.
7. Vein patterns require only low resolution IR. Imaging allied to simple image processing.
8. Vein pattern stability and repeatability requires only simple algorithms for auto identification.
9. Vein structures provide the opportunity for low cost personal worn and pocket biometric keys.
10. Biometric Keys (Biokeys & Biowatches) read wrist or hands dorsal vein structures.
11. Biowatches output encrypted access codes whilst strapped to a recognized non coerced wrist
12. Biokeys & Biowatches output encrypted access codes (Cryptographic signatures) to vehicles, computers, access portals, weapons, firearms etc.
13. Lost Vehicle Biokeys are not a problem; use any other! Vehicle Biokeys default to transmitting unrecognized patterns as plain text.
14. Vehicle security/engine management systems will let you in and drive if they recognize your vein pattern.
15. Biokeys & Biowatches maintain biometric privacy by placing the ownership of the biometric system, data & Crypto keys in the hands of the users.

6.6: Applications of palm vein biometrics [21]

1. Security systems: physical admission into secured areas with oor locks and integrated building security systems
2. Log-in control: network or PC access
3. Healthcare: ID verification for medical equipment, electronic record management
4. Banking and financial services: access to ATM, kiosks, vault
5. Employees time / attendance

7. Previous work on palm veins [20]

The company's palm-vein recognition system has been available in Japan for just over a year and has already achieved some notable success. The Bank of Tokyo Mitsubishi, Japan's third-largest retail bank, began installing the system on its ATMs last October as a higher-security

alternative to personal identification numbers. About half of the bank's 3,000 ATMs will have the system by September, and other major national and regional banks have also said they're adopting the system. The palm-vein detector contains a camera that takes a picture of the palm of a user's hand. The image is then matched against a database as a means of verification. The camera works in the near-infrared range so veins present under the skin are visible, and a proprietary algorithm is used to help confirm identity. The system takes into account identifying features such as the number of veins, their position and the points at which they cross. The result is a system that offers a higher level of security than competing technologies, including voice print, facial recognition, fingerprint recognition and iris scanning, according to Fujitsu. The company's claim is partly based on a real-life test it carried out that involved scanning the hands of 140,000 Fujitsu employees worldwide. The palm-vein technology will be available from Fujitsu in three ways: The company will offer the sensor itself, it will offer a bundle of the sensor and its mPollux authentication software, and it will offer the technology through its system integrator companies direct to customers. An application programming interface will also be available that allows users to add support for the sensor to existing systems. "Fujitsu is very much interested in our palm-based sensor [being] used as a PC or server log-in system," said Toshimitsu Kurosawa, manager of new business development at Fujitsu's Global Business Management unit. Thus the company will target PC and server vendors, he said. Other targets will be system integrators and vendors of specialist systems, like access-control companies or security companies

8. Conclusion and Future Work

Biometrics refers to an automatic recognition of a person based on her behavioral and/or physiological characteristics. Many business applications (e.g. banking) will in future rely on biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made. For instance, fingerprint-based systems have been proven to be very effective in protecting information and resources in a large area of applications. Although companies are using biometrics for authentication in a variety of situations, the industry is still evolving and emerging. At present, the amount of applications employing biometric systems is quite limited, mainly because of the crucial cost-benefit question: supposing biometrics do bring an increase in security, will it be worth the financial cost? The future probably belongs to multimodal biometric systems as they alleviate a few of the problems observed in unimodal biometric systems. Multimodal biometric systems can integrate information at various levels, the most popular one being fusion at the matching score level. Besides improving matching performance, they also address the problem of nonuniversality and spoofing. Finally, we have presented a general view about the most common used biometric systems and choose the palm vein for applying a full system using the advantages of biometrics systems in identify and verify the persons identification, we considered the palm vein is as a good biometric features because of its strong advantages mentioned above, and will try to apply a suitable algorithms to build a system for employees time / attendance. We will use the biometrics feature (palm veins) for employees' time/attendance procedures in different organizations, governmental offices, and companies. A new fast and robust algorithm for processing the collected templates of palm veins will be presented.

References:

[1] http://www.csee.wvu.edu/~ross/pubs/RossBioIntro_CSVT2004.pdf
[2] http://biometrics.cse.msu.edu/
[3] http://www.ee.surrey.ac.uk/icpr2004/tutorials//BiometricRecognition_000.htm
[4] http://www.biometricnewsportal.com/biometrics_definition.asp
[5] http://www.biometricnewsportal.com/hand_biometrics.asp
[6] http://biometrics.cse.msu.edu/CFP/DS36SPIE07.pdf
[7] http://biometrics.cse.msu.edu/publications.html# finger
[8] http://www.fbidrive.com/downloads/FBiWP052005.pdf
[9] http://www.itsc.org.sg/synthesis/2002/biometric.pdf
[10] http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainRossPrabhakar_BiometricIntro_CSVT04.pdf
[11] http://biometrics.cse.msu.edu/Publications General Biometrics / DassZhuJain_ SampleSize_PAMI06 .pdf

[12] http://www.biometricnewsportal.com/signature_biometrics.asp
[13] http://en.wikipedia.org/wiki/Biometrics
[14] http://biometrics.cse.msu.edu/abstracts.html#face3d
[15] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, March/April 2003, pp. 33-42
[16] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004
[17] http://www.findbiometrics.com/Pages/hand_finger%20articles/hand_1.html
[18] Lobna Abouelmaged, " Authentication of E-Learner Based on Sound Signature," M.sc. Thesis, Faculty of Computer Science & Information Systems, Mansoura university, EGYPT, 2009.
[19] http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html
[20] http://www.csoonline.com.au/index.php/id;1478876517;fp;32768;fpid; 61394715
[21] http://www.biometricnewsportal.com/palm_biometrics.asp
[22] http://www.biometricwatch.com/BW_in_print/contactless_palm_vein_ pattern.htm
[23] Hazem M. El-Bakry, "New Fast Principal Component Analysis For Real-Time Face Detection," Accepted for publication in MG&V Journal.
[24] Hazem M. El-Bakry, "New Fast Principal Component Analysis for Face Detection," Journal of Advanced Computational Intelligence and Intelligent Informatics, vol.11, no.2, 2007, pp. 195-201.
[25] Hazem M. El-Bakry, and Nikos Mastorakis, "A New Approach for Fast Face Detection," WSEAS Transactions on Information Science and Applications, issue 9, vol. 3, September 2006, pp. 1725-1730.
[26] Hazem M. El-Bakry, "Faster PCA for Face Detection Using Cross Correlation in the Frequency Domain," International Journal of Computer Science and Network Security, vol.6, no. 2A, February 2006, pp.69-74.
[27] Hazem M. El-Bakry, and Qiangfu Zhao, "Speeding-up Normalized Neural Networks For Face/Object Detection," Machine Graphics & Vision Journal (MG&V), vol. 14, No.1, 2005, pp. 29-59.
[28] Hazem M. El-Bakry, "Human Face Detection Using New High Speed Modular Neural Networks," Lecture Notes in Computer Science, Springer, vol. 3696, September 2005, pp. 543-550.
[29] Hazem M. El-Bakry, and Qiangfu Zhao, "Face Detection Using Fast Neural Processors and Image Decomposition," International Journal of Computational Intelligence, vol.1, no.4, 2004, pp. 313-316.
[30] Hazem M. El-Bakry, and Qiangfu Zhao, "Fast Object/Face Detection Using Neural Networks and Fast Fourier Transform," International Journal on Signal Processing, vol.1, no.3, 2004, pp. 182-187.
[31] Hazem M. El-Bakry, "Face detection using fast neural networks and image decomposition," Neurocomputing Journal, vol. 48, 2002, pp. 1039-1046.
[32] Hazem El-Bakry, "Fast Face Detection Using Neural Networks and Image Decomposition," Lecture Notes in Computer Science, Springer, vol. 2252, December, 2001, pp.205-215.
[33] Hazem M. El-Bakry, "Automatic Human Face Recognition Using Modular Neural Networks," Machine Graphics & Vision Journal (MG&V), vol. 10, no. 1, 2001, pp. 47-73.
[34] Hazem M. El-Bakry, Mohy A. Abou-El-soud, and Mohamed S. Kamel, "A Biometric System For Personal Identification Using Modular Neural Nets, " Mansoura Engineering Journal - Mansoura University - EGPYT, March 2000.
[35] Hazem M. El-bakry, and Mohamed Hamada "Fast Principal Component Analysis for Face Detection Using Cross-Correlation and Image Decomposition," Proc. of IEEE IJCNN'09, Atlanta, USA, June 14-19, 2009, pp. 2296-2303.
[36] Hazem M. El-bakry, and Qiangfu Zhao, "Fast Neural Implementation of PCA for Face Detection," Proc. of IEEE World Congress on Computational Intelligence, IJCNN'06, Vancouver, BC, Canada, July 16-21, 2006, pp. 1785-1790.
[37] Hazem M. El-bakry, "Fast Co-operative Modular Neural Processors for Human Face Detection," Proc. of IEEE World Congress on Computational Intelligence, IJCNN'06, Vancouver, BC, Canada, July 16-21, 2006, pp. 2304-2311.
[38] Hazem M. El-Bakry, "Human Face Detection Using New High Speed Modular Neural Networks," Proc. of 15th International Conf. on Artificial Neural Nets "ICANN

2005", Warsaw, Poland, September 11-15, 2005, pp. 543-550.

[39] Hazem M. El-bakry, and Qiangfu Zhao, "Fast Co-Operative Modular Neural Networks for Fast Human Face Detection," Proc. of IEEE Eighth International Symposium on Signal Processing and its Applications, Sydney, Australia, August 28-31, 2005, pp. 679-682.

[40] Hazem M. El-Bakry, "Fast Neural Networks for Object/Face Detection ," Proc. of 5th International Symposium on Soft Computing for Industry with Applications of Financial Engineering June 28 - July 4, 2004, Sevilla, Andalucia, Spain.

[41] Hazem M. El-Bakry, and Herbert Stoyan "Fast Neural Networks for Sub-Matrix (Object/Face) Detection," Proc. of IEEE International Symposium on Circuits and Systems, Vancouver, Canada, 23-26 May, 2004.

[42] Hazem M. El-Bakry, and Herbert Stoyan "Comments On Using Neural Nets And FFT For Fast Sub-Matrix (Object/Face) Detection," Proc. of Mansoura Fourth International Engineering Conference, 19-22 April, 2004, Sharm El-Sheikh, Egypt.

[43] Hazem M. El-Bakry, and Herbert Stoyan, "Fast Neural Networks for Object/Face Detection," Proc. of the 30th Anniversary SOFSEM Conference on Current Trends in Theory and Practice of Computer Science, 24-30 January, 2004, Hotel VZ MERIN, Czech Republic.

[44] Hazem M. El-Bakry and Herbert Stoyan, "Comments on Fast Multi Scale Object/Face Detection Using MLP and FFT," International Arab Conference of Information Technology, Alexandria, 20-23 Dec., 2003.

[45] Hazem M. El-Bakry, "Comments on Fast Multi Scale Object/Face Detection Using MLP and FFT," Proc. of the Second International Conference on Computational Intelligence, Robotics and Autonomous Systems, 16-18 Dec 2003, Pan Pacific Hotel, Singapore.

[46] Hazem M. El-Bakry, "Comments on Using MLP and FFT for Fast Object/Face Detection," Proc. of the 7th World Multi-Conference on Systemics, Cybernetics and Informatics, 27-30 July, 2003, Orlando, Florida, USA.

[47] Hazem El-Bakry: "Comments on Using MLP and FFT for Fast Object/Face Detection," Proc. of IEEE IJCNN'03, Portland, Oregon, pp. 1284-1288, July, 20-24, 2003.

[48] Hazem El-Bakry "Comments on Using MLP and FFT for Fast Object/Face Detection, " MLMTA 2003: pp.261-264

[49] H. M. El-bakry, "Comments on Using MLP and FFT for Fast Object/Face Detection, " Proc. the Sixth International Conference on Knowledge-Based Intelligent Information & Engineering Systems 16-18 September 2002 Podere d'Ombriano, Crema, Italy.

[50] Hazem El-Bakry "A New Rotation Invariant Algorithm for Face Recognition Using Neural Networks," Proc. of the 6th World Multi-Conference on Systemics, Cybernetics and Informatics, 14-18 July, 2002, Orlando, Florida, USA.

[68] Hazem El-Bakry, "Face Detection Using Neural Networks and Image Decomposition," Proc. of INNS-IEEE International Joint Conference on Neural Networks, 12-17 May, 2002, Honolulu, Hawaii, USA.

[51] Hazem El-Bakry, "Fast Face Detection Using Neural Networks and Image Decomposition," Proc. of the 6th International Computer Science Conference, AMT 2001, Hong Kong, China, December 18-20, 2001, pp.205-215.

[52] H. M. El-bakry, "Fast Cooperative Modular Neural Nets for Human Face Detection," Proc. of IEEE International Conference on Image Processing, 7-10 Oct., 2001, Thessaloniki, Greece.

[53] H. M. El-bakry "A Rotation Invariant Algorithm for Recognition," Proc. of the 7th Fuzzy Days International Conference, Dortmund, Germany, October 1-3, 2001, pp. 284-290.

[54] H. M. El-bakry, "Human Face Detection Using Fast Neural Networks and Image Decomposition," Proc. the fifth International Conference on Knowledge-Based Intelligent Information & Engineering Systems 6-8 September 2001, Osaka-kyoiku University, Kashiwara City, Japan, pp. 1330-1334.

[55] H. M. El-bakry, M. A. Abo-elsoud, and M. S. Kamel, " Fast Modular Neural Networks for Human Face Detection," Proc. of IEEE-INNS-ENNS International Joint Conference on Neural Networks, Como, Italy, Vol. III, pp. 320-324, 24-27 July, 2000.

[56] H. M. El-bakry, M. A. Abo-elsoud, and M. S. Kamel, "Automatic Face Recognition System Using Neural Networks," Proc. of IEEE International Symposium on Circuits and Systems, Geneva, Switzerland, Vol. III, pp. 543-546, May 28-31, 2000.

[57] H. M. El-bakry, and M. A. Abo-elsoud, and M. S. Kamel, "Fast Modular Neural Networks for Face Detection," Proc. of IEEE International Symposium on Circuits and Systems, Geneva, Switzerland, Vol. I, pp. 156-159, May 28-31, 2000.

[58] H. M. El-bakry, M. A. Abo-elsoud, and M. S. Kamel, " Integrating Fourier and PCA with Neural Computing for Face Recognition," Proc. of fhe second International ICSC Symposium on NEURAL COMPUTATION, at the Technical University of Berlin, Germany, pp. 703-708, May 23-26, 2000.

[59] H. M. El-bakry, M. A. Abo-elsoud, and M. S. Kamel, " Integrating Fourier and Wavelet Features with Neural Computing for Face Recognition," Proc. of second International ICSC Symposium on NEURAL COMPUTATION at the Technical University of Berlin, Germany, pp. 518-521, May 23-26, 2000.

[60] Hazem M. El-Bakry, Mohy A. Abo-Elsoud, and Mohamed S. Kamel "A Biometric System For Personal Identification Using Modular Neural Nets, ", The third International Mansoura Engineering Conference, April, 2000.

[61] Hazem M. El-Bakry, Mohy A. Abou-Elsoud, and Mohamed S. Kamel, "Modular Neural Networks for Face Detection,",17th National Radio Conference, Menofiaa, Feb. 22-24, 2000.

[62] Hazem M. El-Bakry, Mohy A. Abou-Elsoud, and Mohamed S. Kamel, "Integrating Fourier Descriptors and PCA with Neural Networks for Face Recognition,", 17th National Radio Conference, Menofiaa, Feb. 22-24, 2000.

[63] H. M. El-bakry, and Mohy A. Abo-Elsoud, "Automatic Personal Identification Using Neural Nets," The 24th international Conference on Statistics, Computer Science, and its applications, pp. 405-416, Cairo, Egypt, 1999.

[64] H. M. El-bakry, and M. A. Abo-elsoud, and M. S. Kamel, "Automatic Face Recognition Using Neural Networks," Proc. of the 12th International Conference on Microelectronics, pp. 105-108, 22-24 Nov., 1999, Kuwait.

[65] Hazem M. El-Bakry and Mohy A. Abo-Elsoud, "Human Face Recognition Using Neural Networks, ", 16th National Radio Conference, Ain Shams University, Feb. 23-25, 1999.

[66] Hazem M. El-Bakry, "Human Iris Detection Using Fast Cooperative Modular Neural Nets and Image Decomposition," Machine Graphics & Vision Journal (MG&V), vol. 11, no. 4, 2002, pp. 498-512.

[67] Hazem M. El-Bakry "Fast Iris Detection for Personal Verification Using Modular Neural Networks," Lecture Notes in Computer Science, Springer, vol. 2206, October 2001, pp. 269-283.

[68] H. M. El-Bakry "Fast Iris Detection for Personal Verification Using Modular Neural Networks," Proc. of the 7th Fuzzy Days International Conference, Dortmund, Germany, October 1-3, 2001, pp. 269-283.

[69] H. M. El-bakry, "Human Iris Detection for Personal Identification Using Fast Modular Neural Nets, " Proc. of the 2001 International Conference on Mathematics and Engineering Techniques in Medicine and Biological Sciences, pp. 112-118, 25-28 July, 2001, Monte Carlo Resort, Las Vegas, Nevada, USA.

[70] H. M. El-bakry, "Human Iris Detection for Information Security Using Fast Neural Nets, " Proc. of the 5th World Multi-Conference on Systemics, Cybernetics and Informatics, 22-25 July, 2001, Orlando, Florida, USA.

[71] H. M. El-bakry, "Human Iris Detection Using Fast Cooperative Modular Neural Nets," Proc. of INNS-IEEE International Joint Conference on Neural Networks, pp. 577-582, 14-19 July, 2001, Washington, DC, USA.

[72] H. M. El-bakry, "Fast Iris Detection Using Neural Nets," Proc. of the 14th Canadian Conference on Electrical and Computer Engineering, pp.1409-1415, 13-16 May, 2001, Canada.

[73] H. M. El-bakry, "Fast Iris Detection for Personal Identification Using Modular Neural Networks," Proc. of IEEE International Symposium on Circuits and Systems, Vol. III, pp. 581-584, 6-9 May, 2001, Sydney, Australia.

[74] H. M. El-bakry, "Fast Iris Detection Using Cooperative Modular Neural Networks," Proc. of the 5th International Conference on Artificial Neural Nets and Genetic Algorithms, pp. 201-204, 22-25 April, 2001, Sydney, Czech Republic.

[75] H. M. El-bakry, "Fast Iris Detection Using Modular Neural Nets," Proc. of the 12th International Conference on Microelectronics, pp. 223-226, 31 Oct.- 2 Nov., 2000, Iran.

[76] H. M. El-bakry, "Fast Iris Detection using Cooperative Modular Neural Nets," Proc. of the 6th International Conference on Soft Computing, 1-4 Oct., 2000, Japan.

[77] H.H.Soliman, A.atwan, and Abd elnasser Saber," Biometric Identification Using palm vein Recognition," Mansoura Journal for Computer Science and Information Systems, Vol4, No. 4, Jan 2008.

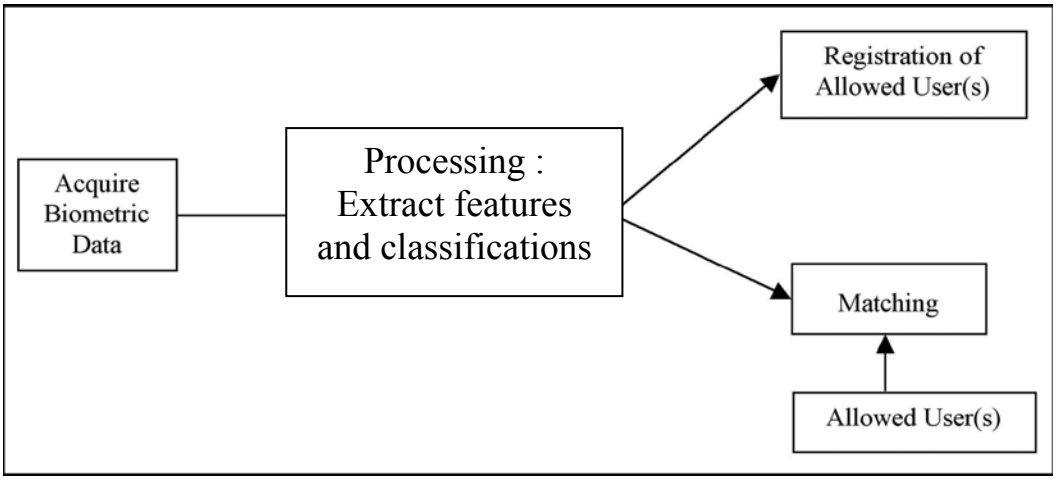

Figure 1: The common process flow of biometrics [3]

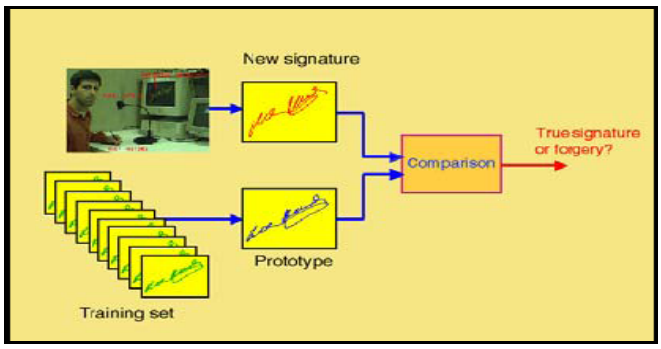

Figure 2: Processing of signature images [12]

Figure 3: Offline Signature

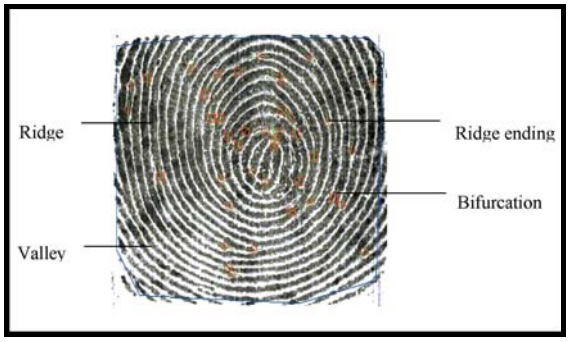

Figure 4: Fingerprint image [7]

Figure 5: Fingerprint scanner [7]

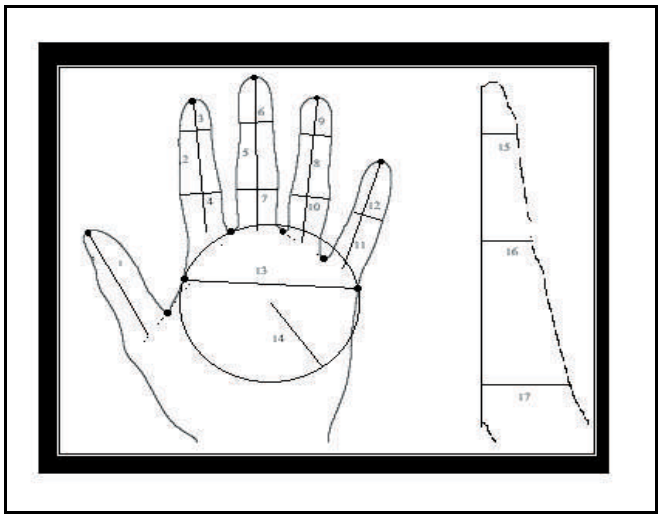

Figure 6 : Hand and finger geometry [5]

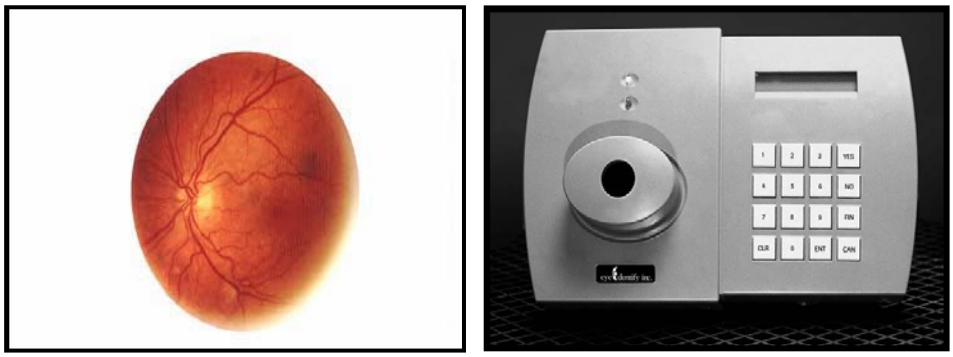

Figure 7: Patterns formed by the blood vessels in the retina of the eye and retina scanning device [11]

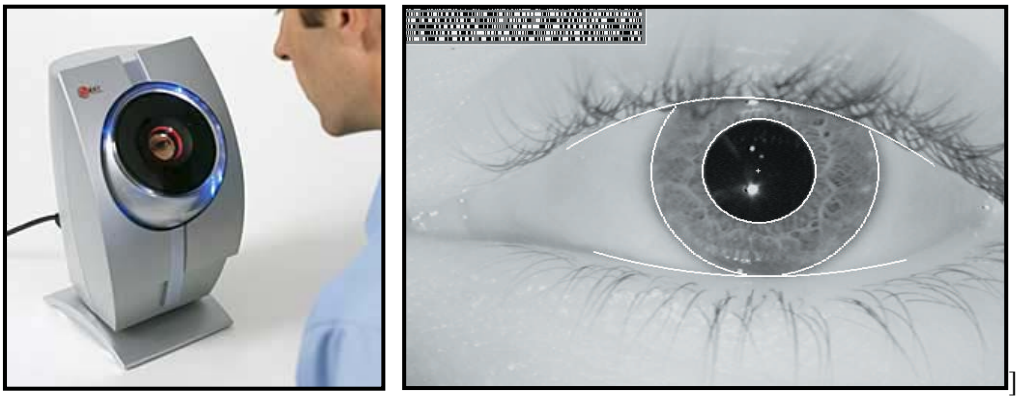

Figure 8: A sample segmented Iris with Iris Code at Top Left Corner and iris scanning device [11]

Figure 9: Personal identification through ear recognition

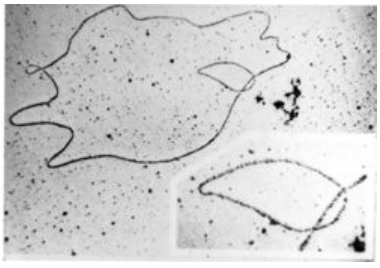

Figure 10: Analysis of a sperm [11]

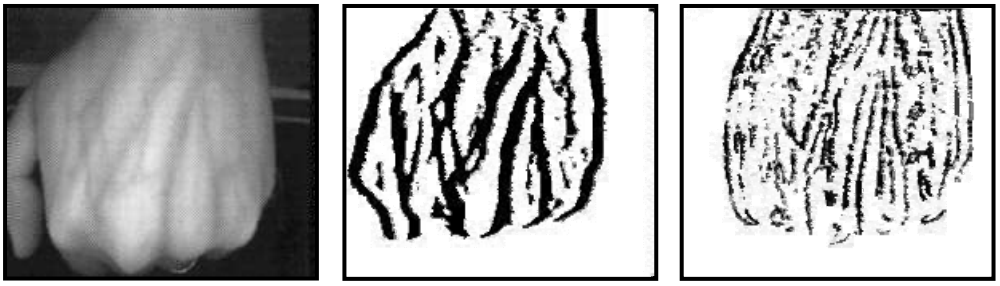

Figure 11 : images of hand veins [19]

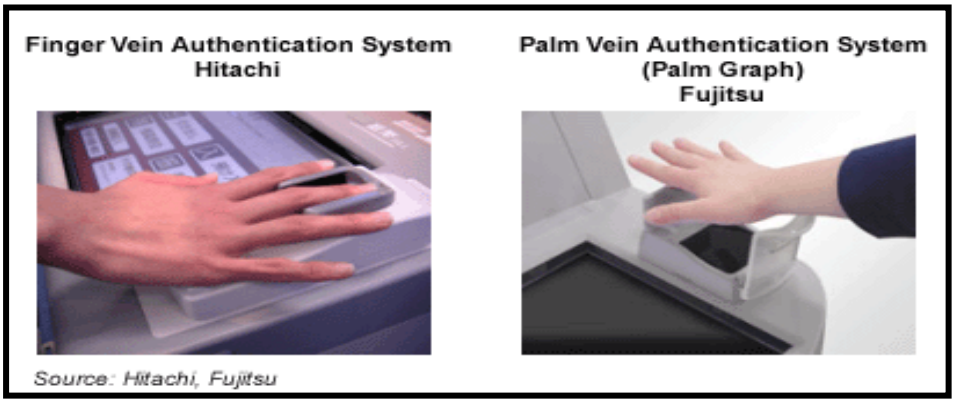

Figure 12 : Palm vein authentication system (palm graph) and finger vein authentication system [19].

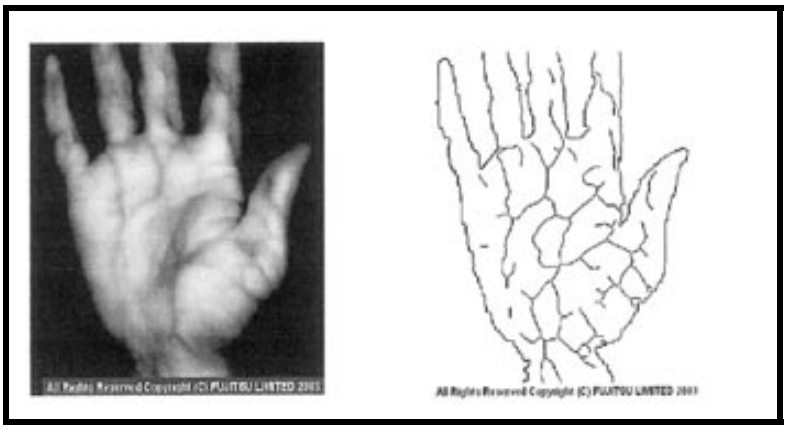

Figure 13. Scan for the palm veins of the human hand [22].

Biometric	*Verify*	*ID*	*Accuracy*	*Reliability*	*Error Rate*	*Errors*	*False Pos.*	*False Neg.*
Fingerprint	√	√	□ □ □ □	► ► ►	1 in 500+	dryness, dirt, age	Ext. Diff.	Ext. Diff.
Facial Recognition	√	×	□ □ □	► ►	no data	lighting, age, glasses, hair	Difficult	Easy
Hand Geometry	√	×	□ □ □	► ►	1 in 500	hand injury, age	Very Diff.	Medium
Speaker Recognition	√	×	□ □	►	1 in 50	noise, weather, colds	Medium	Easy
Iris Scan	√	√	□ □ □ □	► ► ►	1 in 131,000	poor lighting	Very Diff.	Very Diff.
Retinal Scan	√	√	□ □ □ □	► ► ►	1 in 10,000,000	glasses	Ext. Diff.	Ext. Diff.
Signature Recognition	√	×	□ □	►	1 in 50	changing signatures	Medium	Easy
Keystroke Recognition	√	×	□	►	no data	hand injury, tiredness	Difficult	Easy
DNA	√	√	□ □ □ □	► ► ►	no data	none	Ext. Diff.	Ext. Diff.

Biometric	*Security Level*	*Long-term Stability*	*User Acceptance*	*Intrusive*	*Ease of Use*	*Low Cost*	*Hardware*	*Standards*
Fingerprint	► ► ►	»»»	□□	Somewhat	□□□	√	Special, cheap	Yes
Facial Recognition	► ►	»»	□□	Non	□□	√	Common, cheap	?
Hand Geometry	► ►	»»	□□	Non	□□□	×	Special, mid-price	?
Speaker Recognition	► ►	»»	□□□	Non	□□□	√	Common, cheap	?
Iris Scan	► ► ►	»»»	□□	Non	□□	×	Special, expensive	?
Retinal Scan	► ► ►	»»»	□□	Very	□	×	Special, expensive	?
Signature Recognition	► ►	»»	□□	Non	□□□	√	Special, mid-price	?
Keystroke Recognition	► ►	»	□□□	Non	□□□	√	Common, cheap	?
DNA	► ► ►	»»»	□	Extremely	□	×	Special, expensive	Yes

Figure 14. Biometrics Comparison Chart [3]