Vein and Fingerprint Biometrics Authentication- Future Trends

HATIM A. ABOALSAMH

Abstract: - Biometric signatures, or biometrics, are used to identify individuals by measuring certain unique physical and behavioral characteristics. Individuals must be identified to allow or prohibit access to secure areas—or to enable them to use personal digital devices such as, computer, personal digital assistant (PDA), or mobile phone. Virtually all biometric methods are implemented using the following 1) sensor, to acquire raw biometric data from an individual; 2) feature extraction, to process the acquired data to develop a feature-set that represents the biometric trait; 3) pattern matching, to compare the extracted feature-set against stored templates residing in a database; and 4) decision-making, whereby a user's claimed identity is authenticated or rejected. In this paper, a compact system that consists of a CMOS fingerprint sensor (FPC1011F1) is used with the FPC2020 power efficient fingerprint processor ; which acts as a biometric sub-system with a direct interface to the sensor as well as to an external flash memory for storing finger print templates. Distinct Area Detection (DAD) algorithm; which is a feature based algorithm is used by the fingerprint processor, which offer improvements in performance. Vein authentication is another recent advancement in biometrics. Vein biometrics is discussed and comparison with other biometrics is revealed.

Key-Words: - Access control, Vein biometrics, Fingerprint processor, Fingerprint authentication, Biometrics.

I. Introduction

Biometrics technology is based on identification of individuals by a physical or behavioural characteristic. Examples of recognition of physical characteristics are: fingerprints, iris, face or even hand geometry. Behavioural characteristic can be the voice, signature or other keystroke dynamics. What make fingerprints idealistic for personal digital identification is the fact that the fingerprint pattern is composed of ridges and valleys that form a unique combination of distinguishing features of each finger (as shown in Fig.1 ; also, fingerprint characteristics do not vary in time [1]. A comparison of popular biometrics are shown in Tables I and II. From the comparison, it's clear to see why fingerprint and Vein authentication biometrics are attractive alternatives in comparison to other biometrics.

Table I Biometrics Parameters explained

1	**Universality**	each person should have the characteristic.
2	**Uniqueness**	is how well the biometric separates individuals from another.
3	**Permanence**	measures how well a biometric resists aging and other variance over time.
4	**Collectability**	ease of acquisition for measurement
5	**Performance**	accuracy, speed, and robustness of technology used.
6	**Acceptability**	degree of approval of a technology.
7	**Circumvention**	ease of use of a substitute.

Table II Comparison of biometric technologies [4,6]

	Biometrics Parameters						
Biometrics	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Face	high	low	med	high	low	high	low
Fingerprint	med	high	high	med	high	med	high
Hand Geometry	med	med	med	high	med	med	med
Iris	high	high	high	med	high	low	high
Signature	low	low	low	high	low	high	low
Voice Print	med	low	low	med	low	high	low
F. Thermogram	high	high	low	high	med	high	high
Retinal Scan	high	high	med	low	high	low	high
Vein	high	med	med	med	high	med	low

II. Verification and Identification

***Verification* (or *authentication*) systems use fingerprint** technology to *authenticate* the identity of a person. the system receives two inputs: the identity of the person requesting authentication (usually a PIN or smart card) and the scanned fingerprint, as shown in Fig. 1. The PIN is used as a key to retrieve a fingerprint tamplate stored in a database and is compared against the currently offered fingerprint. The verification decision is based on the outcome of the search.

Identification systems identify a person based on a currently scanned fingerprint, as shown in Fig. 2. Such systems receive only one input, namely the live-scanned *query* fingerprint. A database is searched for a matching fingerprint, if a matching fingerprint is found in the database, the search returns a positive outcome otherwise

access is denied. For verification and identification systems, *enrolment* is an important step. This is the process of taking reference (templates) fingerprints of all users and storing these in the database for comparison. [11].

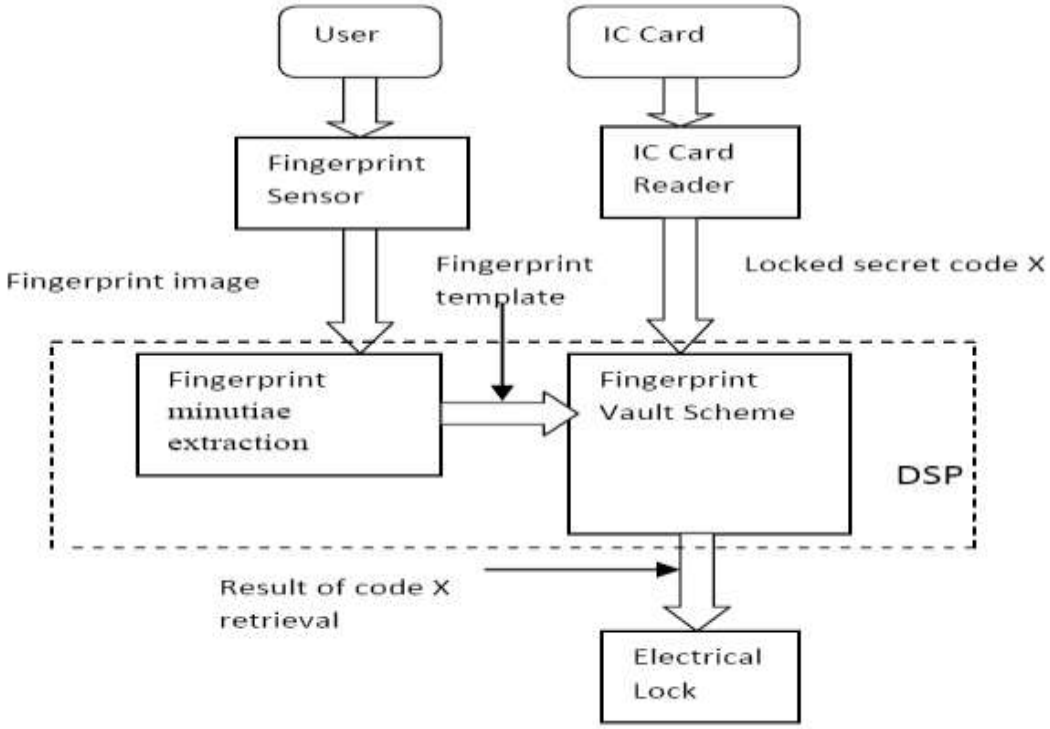

Fig. 1 : A typical fingerprint authentication system

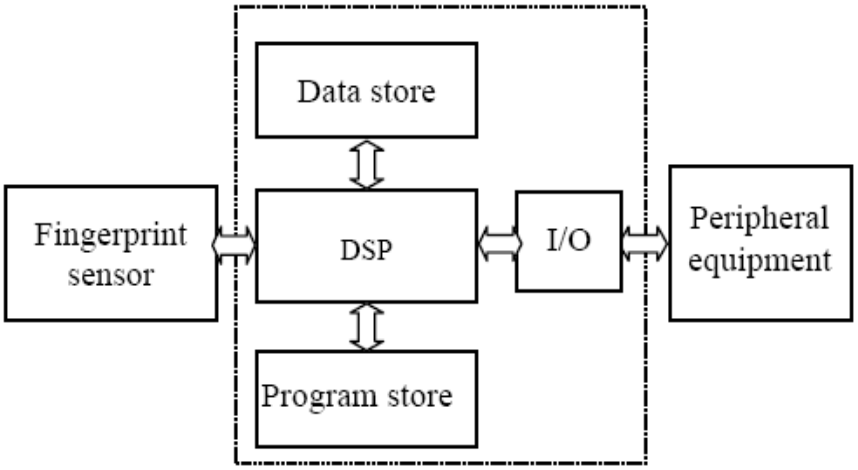

Fig. 2 : A typical Fingerprint Identification system

III. The FPC1011C sensor circuit

A capacitive sensor consists of a two dimensional array of micro-capacitor plates (this resembles image pixels) embedded in a chip (see Fig. 3). The finger skin works as the other side of each micro capacitor plate. Due to distance variations from a ridge on the fingerprint to the sensor and from a valley on the fingerprint to the sensor; variations in electrical charge will appear. This small capacitance difference represents a 2D image of the fingerprint, and is then used to acquire it [9].

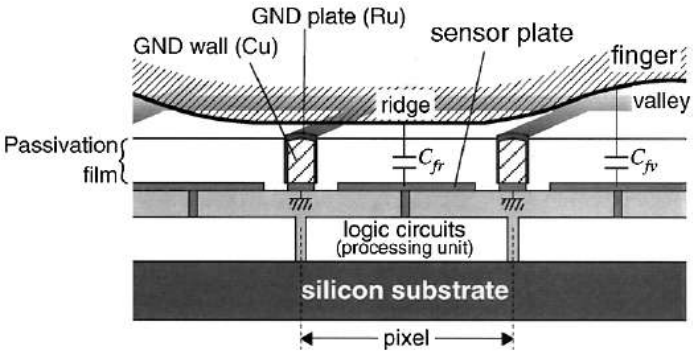

Fig. 3 : sample circuit details of the fingerprint sensor

IV. The FPC2020 Fingerprint processor

The FPC2020 is a small, fast and power efficient ASIC that acts as a biometric sub-system with a direct interface to the FPC1011C sensor as well as to an external FLASH memory for storing templates. Thanks to its small size and low power consumption it fits as well in door locks, card readers and safes as in smaller portable and battery powered devices without losing

identification speed or performance. FPC2020 can easily be integrated into virtually any application and be controlled by a host sending basic commands for enrolment and verification via the serial interface. In a standalone configuration, the processor is not connected to a host, in this case; the application program is pre stored in the FLASH memory connected to the processor. At start-up of FPC2020, a boot sequence (located in ROM) is executed, which downloads the main application code located in the attached FLASH memory, as shown in Fig. 4. If no errors are encountered during this download process, the boot sequence terminates and leaves control to the main application [2]. The FPC2020 processor has over 80 instructions. The instruction set is divided into (7) groups [2]:

1. Biometrics commands
2. Image transfer commands
3. Template Handling Commands
4. Algorithm setting Commands
5. Firmware Commands
6. Communication Commands
7. Other supplementary commands

An example of the FPC2020 processor Template Handling Commands is shown in Table III.

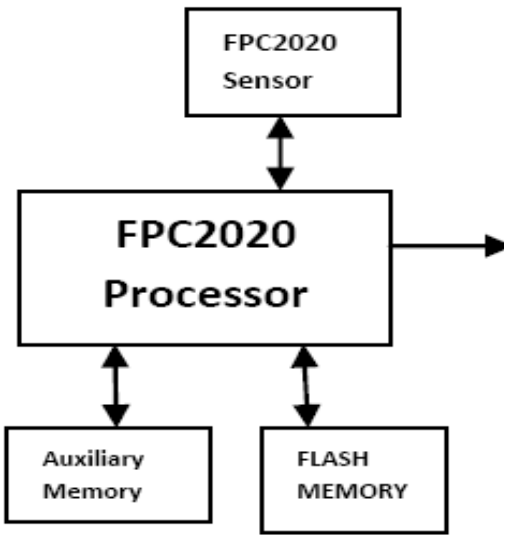

Fig. 4: Biometric sub-system based on the FPC2020 processor and the FPC1011 [2].

Table III Template handling commands [2].

TEMPLATE HANDLING	HEX	DESCRIPTION
API_UPLOAD_TEMPLATE	0xA0	Upload template from RAM
API_DOWNLOAD_TEMPLATE	0xA1	Download template to RAM
API_COPY_TEMPLATE_RAM_TO_FLASH	0xA2	Copy template from RAM to permanent FLASH storage Set slot number in IDX
API_UPLOAD_TEMPLATE_FROM_FLASH	0xA3	Upload template from single FLASH slot Set slot number in IDX
API_DELETE_TEMPLATE_RAM	0xA4	Erase template from RAM
API_DELETE_SLOT_IN_FLASH	0xA5	Delete single slot in FLASH Set slot number in IDX
API_DELETE_ALL_IN_FLASH	0xA6	Delete all FLASH slots
API_DOWNLOAD_TEMPLATE_TO_FLASH	0xA7	Download a template to FLAS

A. Distinct Area Detection (DAD) Built-in algorithm

The FPC2020 (FPC) processor uses a patented Distinct Area Detection (DAD) algorithm; which is a feature based algorithm, looking for features that are unique in its surroundings. It locates distinct areas in and takes full advantages of the three-dimensional full greyscale fingerprint image derived from the FPC1011F1 fingerprint sensor, compared to a simple two-dimensional black and white image. This is shown in Fig.5 , as a comparison with the 2D Minutia based algorithm [3,5].

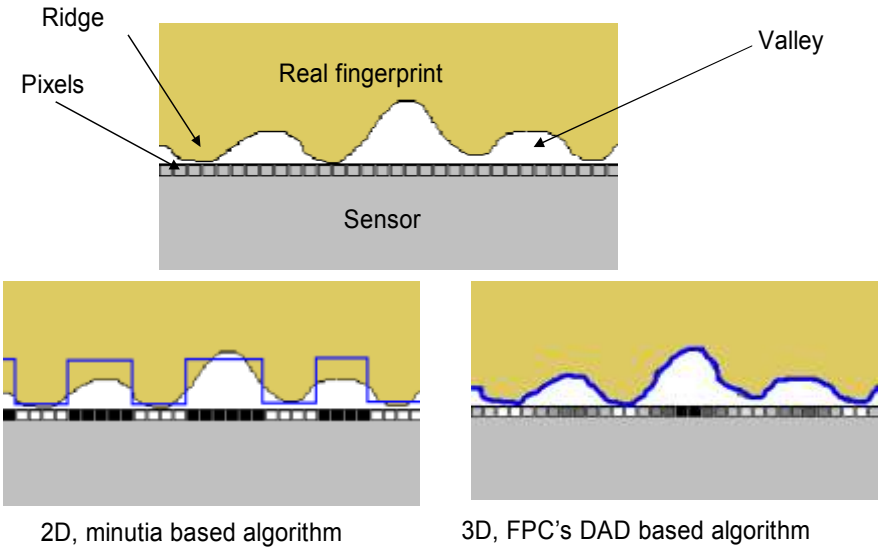

Fig. 5: 2D Minutia Vs 3D DAD Algorithms [8].

A 2D fingerprint has fewer details than a 3D fingerprint representation that the sensor provides. Using image processing techniques, the 3D scan is flattened as shown in Fig. 6 to obtain more features from the image.

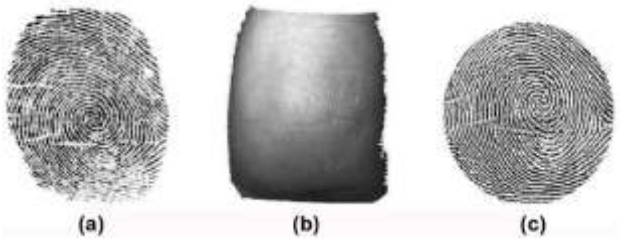

Fig. 6: A finger print scan shows a) A 2D fingerprint, b) A 3D fingerprint scan, and c) a flattened 2D obtained from the 3D scan [13].

In fingerprint recognition, fingerprints are not distinguished by their ridges and valleys, but by elements called Minutia, which are some abnormal points on the ridges as shown in Fig. 7. There are many types of minutia reported in literature [12], two are mostly significant: one is called termination, that represents the immediate ending of a ridge; the other is called bifurcation, which represents the point on the ridge from which two branches derive[12].

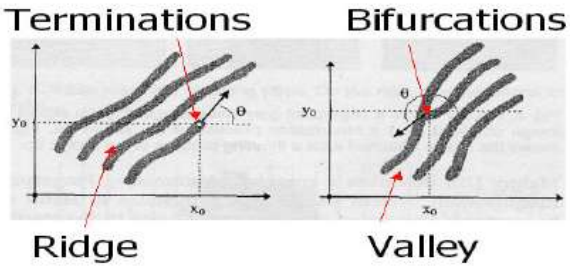

Fig. 7: , the minutiae are indicated with small circles. [11]

In fingerprint recognition, the *minutiae* provide the details of the ridge-valley structures. Automatic fingerprint recognition systems use the two elementary types of minutiae that exist, being ridge endings and bifurcations. Sometimes composite types of minutiae such as lakes or short ridges are also used. In Figure 8 the minutiae are indicated with small circles. [11]

Fig. 8 : Minutiae are extracted and saved as a template to represent the fingerprint

In a minutia based algorithms **template-to-template** authentication is used. After the fingerprint is enrolled, a tamplet-1 is created, then for verification another template-2 is created; then the two templates are compared for matching. The FPC's DAD-algorithm use **Fingerprint-to-template** matching. In this scheme; the fingerprint is enrolled in a template. For verification the extracted features of the fingerprint is compared immediately with the saved template; as shown in Fig.9 [8].

V. Finger Vein Biometric Technology Introduction

In visible light, the vein structure on the back of the hand is not easily discernible. The visibility of the vein structure varies significantly depending on factors such as age, levels of subcutaneous fat, ambient temperature and humidity, physical activity, and hand position. In addition a multitude of other factors including surface features such as moles, warts, scars, pigmentation and hair can also obscure the image. Fortunately, the use of thermo graphic imaging in the near IR spectrum exhibit marked and improved contrast between the subcutaneous blood vessels and surrounding skin, and eliminates many of the unwanted surface features [10].

Based on the patterns of veins in one's finger or hand, vascular pattern recognition (VPR) provides the ease of use with accuracy, smaller readers and contactless use. Finger vein system scans the veins one's fingers and then matches the vein patterns of their respective pre-saved templates.

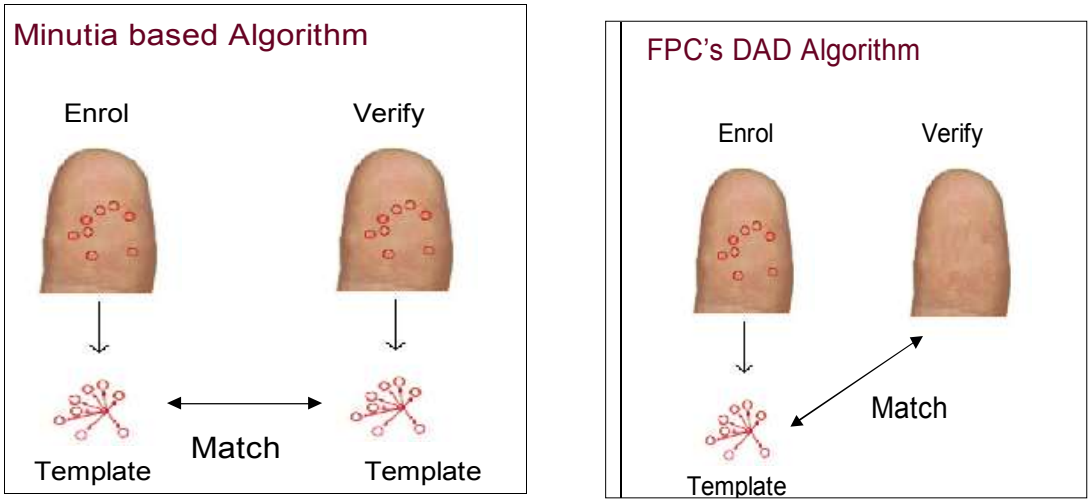

Fig. 9: The Minutia Algorithm Vs DAD-algorithm [8].

A set of LEDs (light emitting diodes) generates near infrared light that penetrates the body Tissue. An image of the veins pattern is revealed as the near infrared light is reflected in the haemoglobin in the blood. A CCD (charge coupled device) camera uses a small, rectangular piece of silicon to receive incoming light. The CCD captures the image of the vein pattern through this reflected light. The Image is processed through an algorithm to constructs a finger vein pattern from the camera image. This pattern is then digitized and saved as a template for biometric authentication, as shown in Figure 10.

Finger vein FV systems have some very powerful advantages [7]:

1. There is no property of latency. The vein patterns in fingers stay where they belong, and where no one can see them – in the fingers. This is a huge privacy consideration.
2. Vascular sensors are both durable and usable. The sensors are looking below the skin; and they simply don't have issues with finger cuts, moisture or dirt.
3. Finger vein systems demonstrate very high accuracy rates, currently higher than fingerprint imaging, and they are very difficult to spoof; however, the relative accuracy of the two technologies could change over time since fingerprint technology has been making significant improvements.
4. The finger vein systems are near contactless. What that means is that only the very top of the finger makes contact; and that is just to align the finger for consistent imaging. The middle part of the finger (the middle phalanx) from where the CCD camera captures its image has no surface contact with anything.
5. Finger vein systems are extremely easy to use as they are fairly intuitive and require very little training on the part of the user.

A. Procedure for personal identification

The procedure for personal identification by using patterns of veins in a finger is shown in Fig. 1. The details are described below [10].

Step 1: Acquisition of an infrared image of the finger
A special imaging device is used to obtain the infrared image of the finger. An infrared light irradiates the backside of the hand and the light passes through the finger. A camera located in the palm side of the hand captures this light. The intensity of light from the LED is adjusted according to the brightness of the image.. As haemoglobin in the blood absorbs the infrared light, the pattern of veins in the palm side of the finger are captured as shadows. Moreover, the transmittance of infrared light varies with the thickness of the finger. Since this varies from place to place, the infrared image contains irregular shading. In Fig. 2, b and c are examples of the captured images.

Each image is greyscale, 240 × 180 pixels in size, with 8 bits per pixel. The length of the finger is in the horizontal direction, and the fingertip is on the right side of the image.

Step 2: Normalization of the image the location and angle of the finger in the image require some form of normalization, since these qualities will vary each time. Two-dimensional normalization is done using the outline of the finger on the assumption that the three-dimensional location and angle of the finger are constant.

Step 3: Extraction of finger-vein patterns the finger-vein pattern is extracted from the normalized

As shown in Fig 13, the process of locating the veins through greyscale searching continues until a skeleton of the vein pattern is formed. The vein formed pattern is then saved as a template to be stored in a database and uniquely associated with an individual, as shown in Fig. 13.

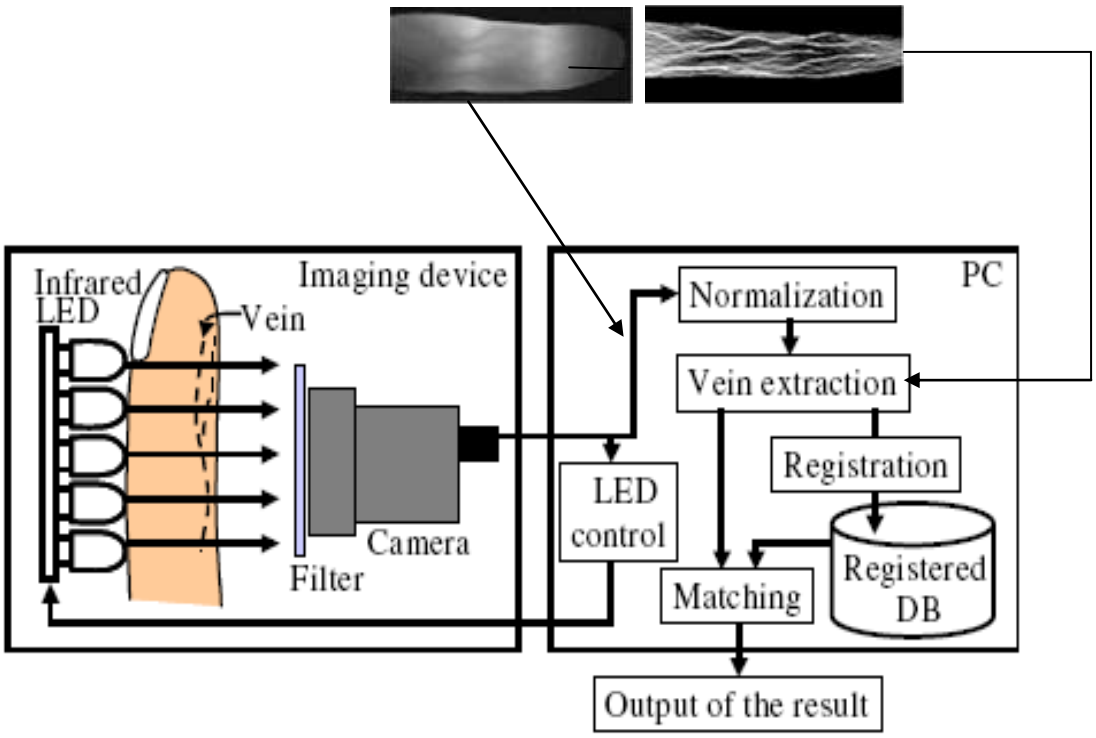

Fig.10 : Feature extraction of finger-vein patterns [14]

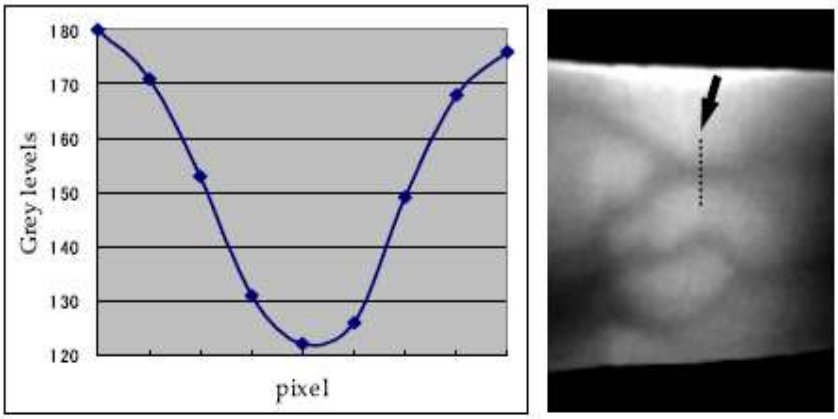

Fig. 11: a vein search in (b) uses pixels greyscale value in (a) to determine the structure of the vein [10].

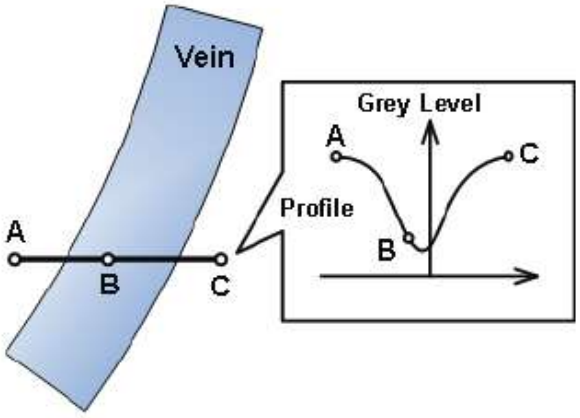

Fig 12 : process of locating the veins through greyscale searching [14].

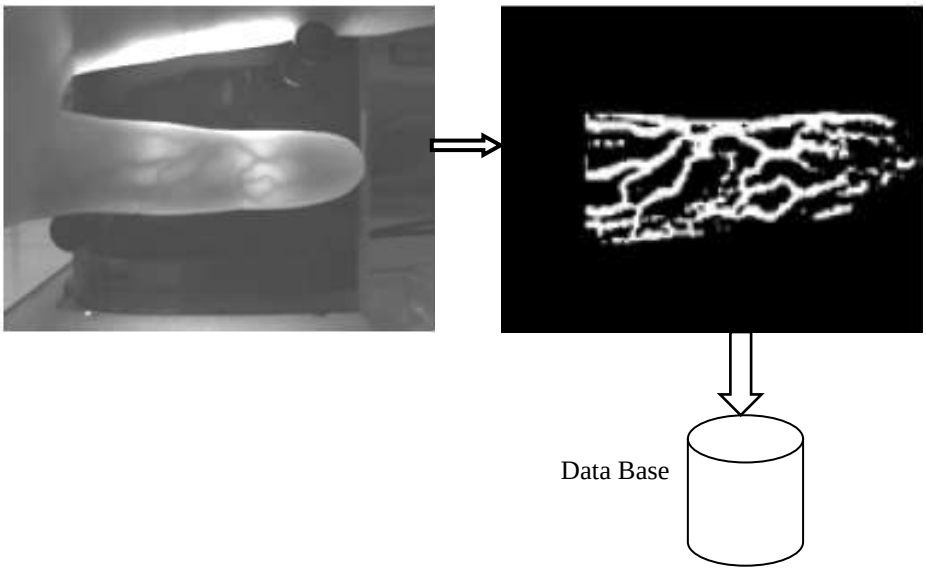

Fig. 13: Results for extracted finger veins into a template for matching process.

VI. Conclusions

To reduce the size of a fingerprint biometric system, a CMOS sensor-chip is used. The FPC1011F1 fingerprint sensor Package connected to the FPC2020 fingerprint processor; which acts as a biometric sub-system with a direct interface to the sensor as well as to an external flash memory for storing templates. The small size and low power consumption enables this integrated device to fit in card readers and in smaller portable and battery powered devices without losing identification speed or performance. Hence; the proposed system will save time since it has one matching operation to perform, and will save cost since no external fingerprint readers are needed. Although the FPC1011F1 fingerprint sensor is designed especially for the FPC2020 dedicated fingerprint processor; (which means that no additional interfacing circuit is needed); our further work will include interfacing the FPC2020 dedicated fingerprint processor with other sensors[5], and comparing cost, interface, size, performance, and ergonomics of the design.

Vein identification is another promising biometrics. Advantages of vein biometric was revealed in this paper, yet; many factors could affect the quality of the veins image such as the amount of blood flow in the veins .Image processing

techniques are essential in enhancing the vein image in preparation for digitization and preparation of the templates. Different image processing and enhancement algorithms will be applied to the row vein images under different condition, to compare performance and reliability of authentication in our future work.

References:

[1] Salah M. Rahal, Hatim A. Aboalsamh, Khalid N. Muteb, Multimodal Biometric Authentication System- MBAS, *2nd IEEE International Conf. On Communication & Technologies: From Theory to Applications*, , April 24-28, 2006, Vol. 1, 24-28, pp. 1026-1030.

[2] The FPC1011F1 Area sensor, FPC2020 fingerprint processor Package product specifications, www.fingerprints.com

[3] W.L. WOO , S. S. DLAY, **A** Novel Biometric Fingerprint Pressure Deformation Algorithm, *Proceedings of the 5th WSEAS Int. Conf. on SIGNAL, SPEECH and IMAGE PROCESSING*, Corfu, Greece, August 17-19, 2005, pp80-83.

[4] Yigang ZhangI, Qiong Li, Xinguang Zou, Kecheng Hao, Xiamu Niu, The Design of Fingerprint Vault Based IC Card Access Control System, *Proceedings of the 5th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications*, Madrid, Spain, February 15-17, 2006, pp172-175.

[5] Majid Meghdadi, Saeed Jalilzadeh, Validity and Acceptability of Results in Fingerprint Scanners, *7th WSEAS Int. Conf. on MATHEMATICAL METHODS and COMPUTATIONAL TECHNIQUES IN ELECTRICAL ENGINEERING*, Sofia, October 27-29 2005, pp259-266.

[6] A. K. Jain, A. Ross, and S. Prabhakar, An Introduction to Biometric Recognition , IEEE Trans. on Circuits and Systems for Video Technology, Issue 14, Volume 1, 2004, pp. 4-19.

[7] Liukui Chen, Hong Zheng, Personal Identification by Finger Vein Images Based on Tri-value Template Fuzzy Matching, *WSEAS TRANSACTIONS on COMPUTERS*, Issue 7, Volume 8, July 2009, pp1165-1174.

[8] Fingerprint Cards AB, Corp., Gothenburg, Sweden, http://www.fingerprints.com/Technology/Sensors%20and%20algorithms.aspx

[9] Eric K. Y. Chan and John A. Pearce, A Computer assisted thermography system for the extraction, visualization and tracing of subcutaneous peripheral venous patterns, *IEEE International Symposium on Circuits and Systems*, 1991, pp 508 –511.

[10] Naoto Miura, Akio Nagasaka, Takafumi Miyatake, Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification, *Machine Vision and Applications* ,2004 ,pp 194–203.

[11] Asker M. Bazen, Fingerprint Identification - Feature Extraction, Matching, and Database Search *Masters of Technology. Thesis*, Punjabi University, August, 2002.

[12] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu, Fingerprint Verification System using Minutiae Extraction Technique, *World Academy of Science, Engineering and Technology* 46, 2008, pp 497-502.

[13] YongchangWang, Laurence Hassebrook, and Daniel Lau, Noncontact, depth-detailed 3D Fingerprinting, *SPIE News Room report, 2009* .

[14] Li Xueyan and Guo Shuxu,The Fourth Biometric - Vein recognition, *Pattern Recognition Techniques, Technology and Applications*, pp. 537-546.