A Multi Biometric System Using Combined Vein and Fingerprint Identification

Hatim A. Aboalsamh

Abstract*:* 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 fingerprint sensor as well as to an external PC for storing finger print templates. Added to the fingerprint system is a vein image extraction system; it consists of a set of LEDs (light emitting diodes) that 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. The integrated system will extract two biometrics identifiers; namely, vein and fingerprint. Multi-biometric fusion stages are pointed out; and future research issues are suggested.

Keywords: Access control, , Fingerprint processor, Fingerprint authentication, Vein biometrics, Multi- biometrics. Multi-biometrics fusion.

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 biometrics are both an attractive alternative in comparison to other biometrics.

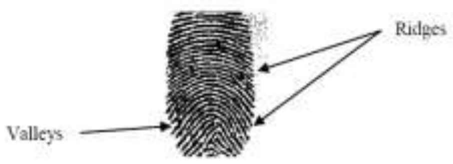


Fig. 1: An illustration of Ridges and Valleys in finger prints

Table I Biometrics parameters explained

	Biometrics parameters	Meaning
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 parameters for different biometric technologies

	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

Vein pattern biometrics is another unique feature to identify individuals. The vein patterns could be obtained from fingers or the whole palm. The equipments used to obtain an image of the vain pattern are also simple and inexpensive. Image processing techniques are capitalized on to provide template creation and, at a later phase, pattern matching [14].

II. SYSTEM COMPONINTS FOR FINGERPRINT DENTIFUICATION

The fingerprint system is divided into two main components: the fingerprint sensor, and the fingerprint processor. The following subsections details those components.

A. The fingerprint sensor selection

One of the most important tasks considering an automatic fingerprint biometric recognition system is the biometric pattern extraction from the captured image of the fingerprint. Due to imperfections of the acquired image, in some cases certain pattern can be missed by the extraction algorithm. Image imperfections can also generate errors in determining the coordinates of each true pattern and its relative orientation of the image. All these facts make remarkable decrease of the recognition system reliability [7]. Thus, an efficient and reliable fingerprint scanning apparatus is an essential component of the whole system.

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], as shown in Fig.4.

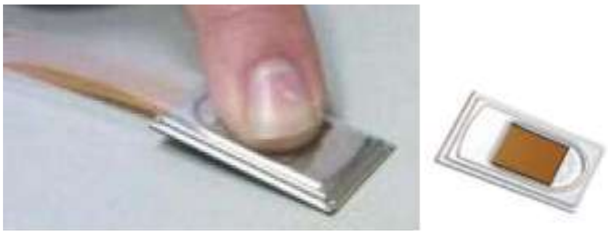


Fig. 3: The FPC1011F1 compact CMOS fingerprint sensor [2].

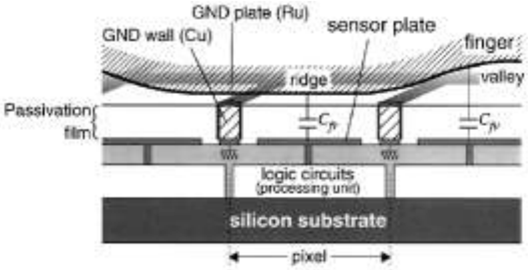


Fig. 4: Capacitive fingerprint sensor.

The FPC1011F1 is a new compact CMOS capacitive fingerprint sensor with several significant advantages. The FPC1011F1 delivers superior image quality, with 256 gray scale values in every single pixel. The reflective measurement method sends an electrical signal via the frame directly into the finger. This technique enables the use of an unbeatably hard and thick protective surface coating. The sensor with its 3D pixel sensing technology can read virtually any finger; dry or wet. With the new hard and durable surface coating, FPC1011F1 is protected from high static voltage, as well as impact and scratches. A cross section of the capacitive sensor is shown in Fig. 4.

2. Architecture of the FPC1011F1 fingerprint sensor Package

As shown in Fig. 5, the sensor package consists of several vital components to read the fingerprint and transform the reading into a greyscale representation of the fingerprint. The readout is then stored in a serial flash memory as a template.

The sensor area is a matrix of 152x200 elements that represent pixels. Once the finger is positioned over the sensor, a voltage is supplied and moved through the finger to the elements of the sensor matrix. Each matrix will hold a voltage value. Those values are deferent, since they represent ridges and valleys of the fingerprint. The sensor element values are transferred in sequence through the X and Y address registers. Each sensor element is converted through an A/D circuit to a digital value that represents a gray scale pixel (values between 0 and 255). The pixels are then transferred to a serial flash memory and organized into a template. The memory template represents a gray scale image of the fingerprint [2].

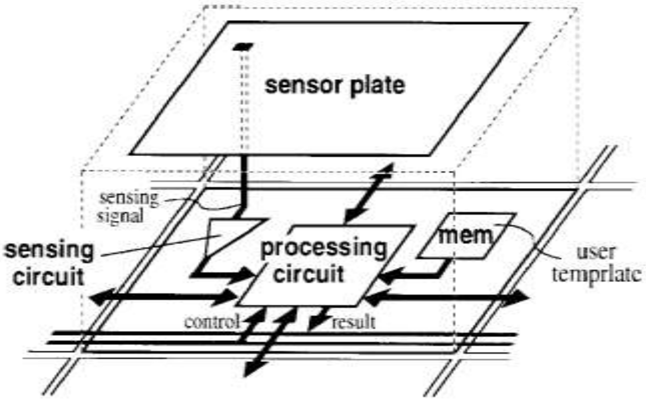


Fig. 5: Data Acquisition process of one pixel of the FPC1011F1 fingerprint sensor .

The sensor matrix consists of 152 x 200 sensor elements. The entire sensor, or a part of it, is read by applying a read sensor instruction. The size of the active area is set by the values of the X and Y registers. The default values for these registers select the complete sensor area to be read once. The readout sequence is illustrated in Fig. 6. During all read operations, 8 pixels are captured simultaneously. By default the first 8pixels being read are pixel (0,0) to (7,0),followed by pixels (8,0) to (15,0).

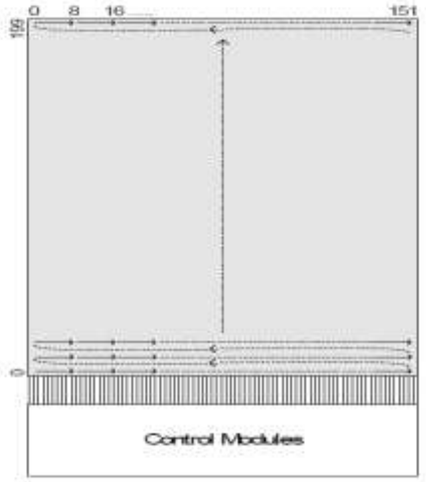


Fig. 6: The readout sequence of the fingerprint sensor [2]

B. The Fingerprint Processor Selection

Many systems attempted to create single chip fingerprint recognition. An example of such system is the Blackfin RISC processor connected to the AT77C104B FingerChip IC . The fingerChip IC captures the image of a fingerprint as the finger is swept vertically over the sensor window. This type of sensor is effective [11], but not suitable ergonomically; since it require the finger to be swapped over the sensor.

The Blackfin processor is a general purpose processor; that means that an application program to do the fingerprint image feature extraction, and other necessary operation; must be provided by the system designer. This prompted us to search for a more designer friendly system. Such a processor will perform fingerprint image feature extraction using one single command.

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. If no errors are encountered during this download process, the boot sequence terminates and leaves control to the main application. This is the default behaviour, which typically always should occur in the standard set-up.

The boot sequence takes 180 ms. The Fingerprint templates are created automatically and stored in flash memory connected to FPC2020. Templates used for verification can also be uploaded/downloaded to an external storage, e.g. central database, smart card or portable flash memory. FPC2020 has no internal limitation in number of templates it can handle. Size of external flash memory will set the limitation [3]. The pin out configuration of FPC2020 processor is shown in Fig. 7.

The application program is stored into the auxiliary memory connected to the fingerprint processor. The program start executing once the finger is positioned over the sensor package. The program consists of instructions to read the sensor area and match it with a pre stored (enrolled) fingerprint templates stored in a database by a host computer(pc).

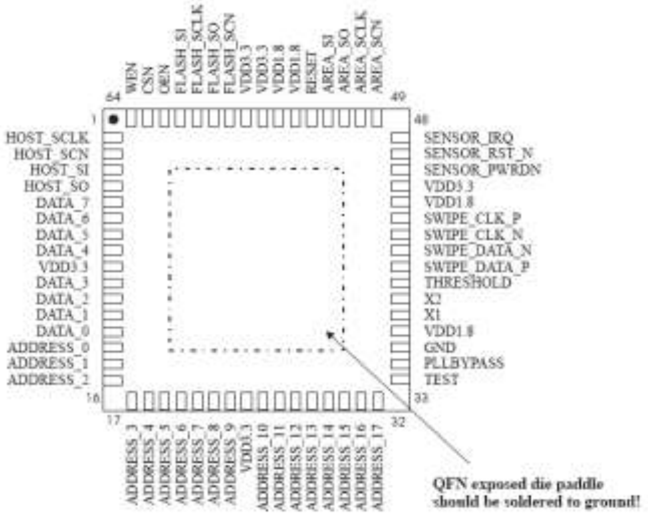


Fig. 7: The 64 pin out configuration of FPC2020 processor [3].

C. The Finger Print Processors instruction set

The FPC2020 processor has over 80 instructions. The instruction set is divided into (7) groups [3]:

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

Instructions from the first group are listed, and their description is shown in Table III as an example [3].

Table III Biometrics commands

BIOMETRIC COMMANDS	HEX	DESCRIPTION
API_CAPTURE_IMAGE	0x80	Capture image from sensor (before enrol).
API_CAPTURE_AND_ENROL_RAM	0x81	Enrol into RAM (includes Capture Image)
API_CAPTURE_AND_VERIFY_RAM	0x82	Verify against RAM (includes Capture Image)
API_CAPTURE_AND_VERIFY_FLASH	0x83	Verify against single FLASH slot (includes Capture Image) Set slot number in IDX
API_CAPTURE_AND_IDENTIFY_FLASH	0x84	Identify against all FLASH slots (includes Capture Image)
API_ENROL_RAM	0x85	Enrol into RAM
API_VERIFY_RAM	0x86	Verify against RAM
API_VERIFY_FLASH	0x87	Verify against single FLASH slot Set slot number in IDX
API_IDENTIFY_FLASH	0x88	Identify against all FLASH slots
API_CAPTURE_IMAGE_FINGERPRESENT	0x89	Capture Image from sensor (once a finger is present)
API_ENROL_FLASH	0x92	Enrol into FLASH memory
API_CAPTURE_AND_ENROL_FLASH	0x93	Enrol into FLASH memory (includes Capture Image)

III. 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, as shown in Fig. 8 [2].

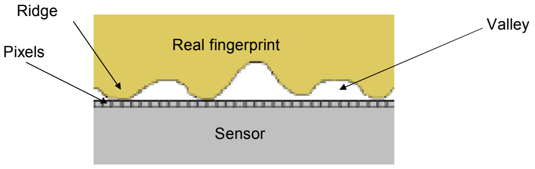


Fig. 8: 3D DAD minutia algorithms[12]

A minutia based algorithms obtains the fingerprint features and store it in a data base (enrol process). In the identification phase a template-to-template matching process is conducted on the database. as shown in Fig. 9.

2D minutia based algorithm 3D FPC's DAD based algorithm

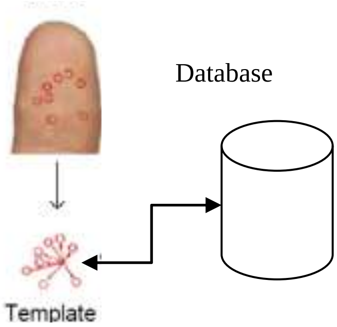


Fig. 9 The minutia algorithm using one templates for enrols and for identify[15].

IV. INCORPORATING FINGER VEIN BIOMETRIC

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 [14].

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.

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 Fig. 10.

Finger vein FV systems have some very powerful advantages [13]:

a. 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.

b. 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.

c. 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.

d. 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.

e. 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 [14].

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 our system, 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. Figure 10 shows how the 3 steps are compound in the system, while Fig. 11 shows a vein search in (b) uses pixels greyscale value in (a) to determine the structure of the vein [14].

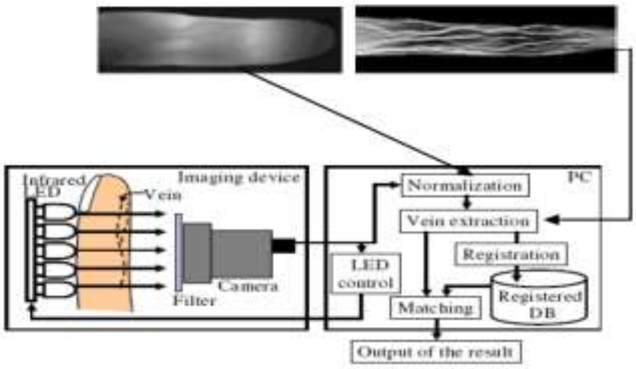
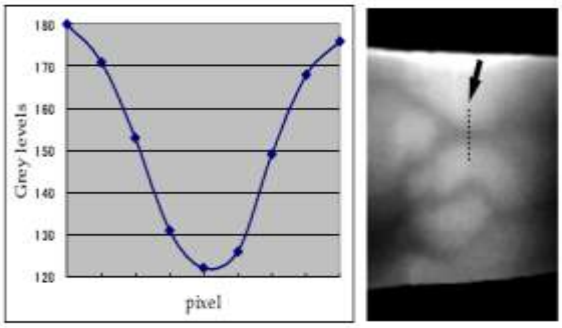


Fig. 10: Results for extracted finger veins into a template for matching process[14].



(a) (b)

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

A vein feature extraction algorithm detects veins through gray scale comparison of the neighbouring pixels, as shown in Fig. 12.

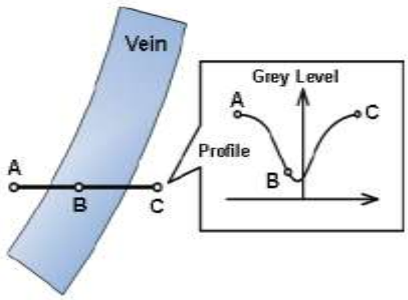


Fig 12 : process of locating the veins through greyscale searching [16].

V. SYSTEM INTEGRATION

The design of the system incorporates two biometrics identifiers, fingerprint and vein patterns. The compact CMOS fingerprint sensor (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 PC for storing templates. The sensor and fingerprint processor is integrated with a vein pattern extraction system that consists of a set of LEDs (light emitting diodes) and a CCD (charge coupled device) camera. An image of the veins pattern is revealed as the near infrared light is reflected in the haemoglobin in the blood. 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 identification. The two templates extracted from the finger (fingerprint and vein pattern) are stored in a database in the enrol phase. In the identification phase, the templates are extracted from the finger and matched with entries in the database to accept or reject the individual. The integrated system's block diagram is shown in Fig.13.

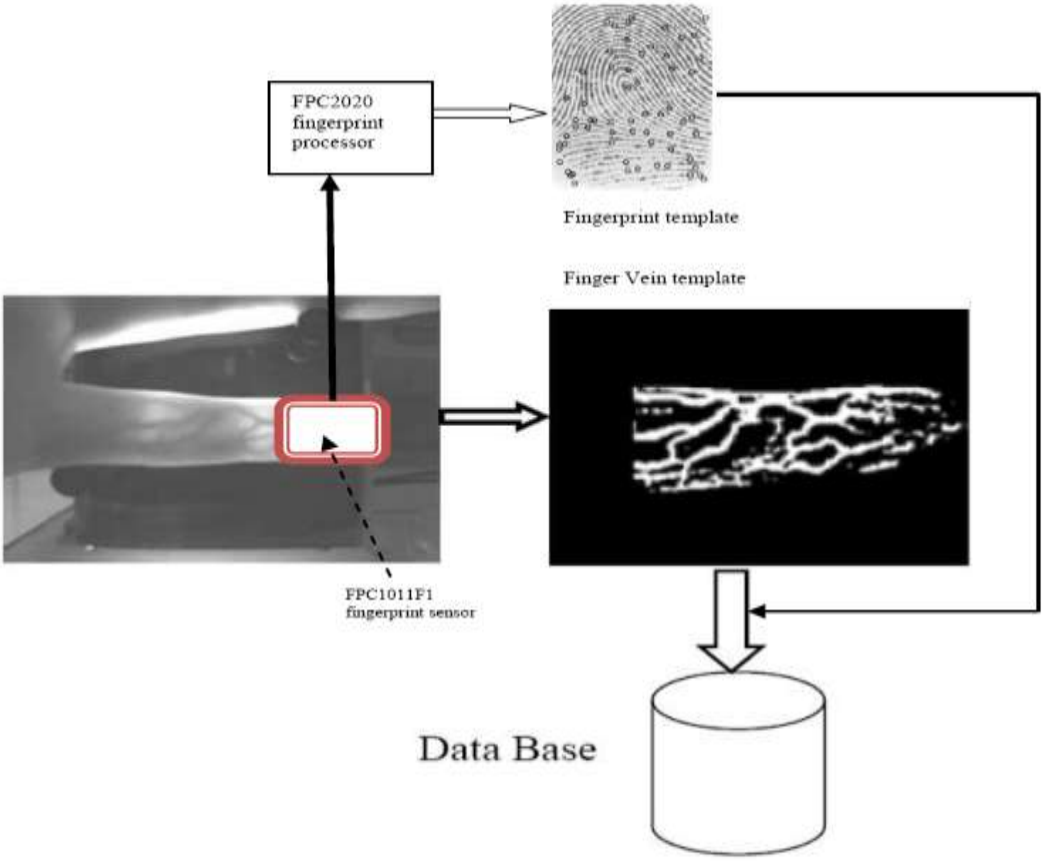


Fig. 13 A block diagram of the vein fingerprint integrated authentication system

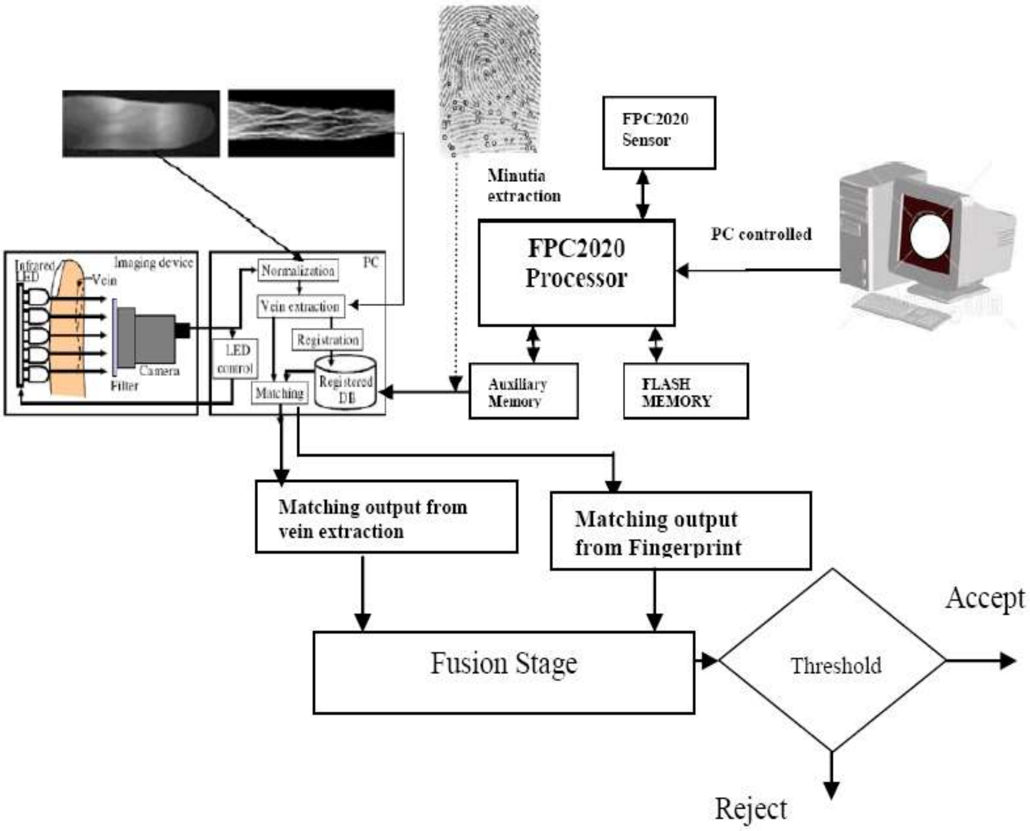


Fig. 14 A detailed diagram of the vein fingerprint integrated authentication system

VI. CONCLUSION

The design of the system uses two biometrics identifiers, fingerprint and vein patterns. The fingerprint sensor FPC1011F1 fingerprint is connected to the FPC2020 fingerprint processor with a direct interface , as well as to an external PC for storing templates. The sensor and fingerprint processor is integrated with a vein pattern extraction system that consists of a set of LEDs that 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 camera receives the 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. The two templates extracted from the finger (fingerprint and vein pattern) are stored in a database in the enrol phase. In the identification phase, the templates are extracted from the finger and matched with entries in the database to accept or reject the individual. Future work will examine different fusion stages , and introduce different thresholds to compare results.

References

[1] S. M. Rahal, H. A. Aboalsamh, K. N. Muteb, “Multimodal Biometric Authentication System- MBAS”, 2nd IEEE International Conf. On Communication & Technologies: From Theory to Applications, , Vol. 1, 24-28, pp. 1026-1030 (2006).

[2] Fingerprint Cards AB, Corp., Gothenburg, Sweden, The FPC1011F1 Area sensor Package product specifications, http://www.fingerprints.com/Products/Sensors.aspx

[3] Fingerprint Cards AB, Corp., Gothenburg, Sweden, The FPC2020 fingerprint processor , http://www.fingerprints.com/Products/Processors.aspx

[4] RFID: Frequency, standards, adoption and innovation, JISC Technology and Standards Watch (2006).

[5] K. Finkenzeller, RFID-Handbook, 2nd edition: Wiley & Sons LTD.(2003).

[6] System Design Guide microID® 125 kHz RFID, Microchip Technology Inc. (2004).

[7] 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, pp80-83 , Corfu, Greece (2005).

[8] Y. ZhangI, Q. Li, X. Zou, K. Hao, X. 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, pp172-175, Madrid, Spain(2006).

[9] M. Meghdadi, S. Jalilzadeh , “ Validity and Acceptability of Results in Fingerprint Scanners”, 7th WSEAS Int. Conf. on MATHEMATICAL METHODS and COMPUTATIONAL TECHNIQUES IN ELECTRICAL ENGINEERING, pp259-266, Sofia, Italy(2005)..

[10] S. Srinivasan, A. Aggarwal, A. Kumar,” RFID Security and Privacy Concerns”, Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, pp69-74, Tenerife, Spain(2005).

[11] J. Addepalli , A. Vasudev, Fingerprint Sensor and Blackfin Processor Enhance Biometric-Identification Equipment Design, Analog Dialogue (2008).

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

[13] L. Chen, H. 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.

[14] N. Miura, A. Nagasaka, T. 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.

[15] M. Kaur, M. Singh, A. Girdhar, and P. S. Sandhu, “Fingerprint Verification System using Minutiae Extraction Technique”, World Academy of Science, Engineering and Technology 46, 2008, pp 497-502.

[16] L. Xueyan and G. Shuxu,”The Fourth Biometric - Vein recognition”, Pattern Recognition Techniques, Technology and Applications, pp. 537-546