On-Line, Low-Cost and Pc-Based Fingerprint Verification System Based on Solid-State Capacitance Sensor

Mohamed. K. Shahin*, Ahmed. M. Badawi**, and Mohamed. S. Kamel**

*B.Sc. Design Engineer at International Electronics, R&D Dept., Cairo, Egypt.
mkhairys@hotmail.com
** Ph.D. Associate Professor of Biomedical Engineering, Cairo Univ., Faculty of Eng., Egypt.
ambadawi99@hotmail.com

***Abstract*- With the recent advancements in the sensor technology and solid-state VLSI design the new capacitance fingerprint sensor can be miniaturized. The Automatic Gain Control (AGC) adjusts the acquired images to produce highest quality images over different dryness, wet and dirty conditions. We developed a low-cost, on-line, and Pc-based fingerprint verification system. The system performance is highly specified which verify in less than one second and enroll in less than a second. The verification system can be used in access control systems, in banking, airport and in attendance system.**

***Keywords*- Solid-state capacitance fingerprint sensor, Minutiae, Thinning, Point matching.**

I. INTRODUCTION

Fingerprints are recognized as one of the most practical methods for positive identification of individuals. This is due to the fact that fingerprint patterns are unique to every individual and to every finger. Fingerprints of even identical twins are different [1]. Fingerprint sensors (scanners) can be categorized into the following types:

A. Off-line sensors:

The first type is the fingerprint acquisition via inking, which is the traditional mode of criminal fingerprint capture. It is evident that this is inappropriate for fingerprint verification due to the inconvenience involved with ink and the need for subsequent digitization.

B. On-line sensors:

An on-line sensor is used for fingerprint verification and is called "live-scan fingerprint capture" and it is divided into 3 sub-types:
1) Ultrasound, 2) Optical and 3) Solid-state fingerprint sensors.

The last one also subdivides into 3 classes thermal, pressure and capacitance sensor. With the recent advancements in sensor technology and solid-state VLSI design the new capacitance fingerprint sensor can be miniaturized [2]. This opens new frontiers for fingerprint-based identification technology in commercial applications. These devices incorporate a sensing surface of about 300X300 pixels with a spatial resolution of about 500 dpi. In spite of the good quality images acquired by the capacitance fingerprint sensor when compared with the other fingerprint sensors the small fingertip area acquired 0.6"X0.6" enters the challenge for incorporating new fingerprint features in addition to the two traditional features: the ridge endings (terminations) and Bifurcations (Fig. 1) in the matching procedure. This is due to the overlapping area may be small for the verification of the same finger (Fig. 2) and it's evident that this is more efficient than reducing the number of minutiae needed for deciding a true match. These features may be minutiae direction and the number of ridges crosses the line between minutia points. Section 2 describes our sensor properties, our fingerprint image processing and pattern processing modules are entailed in section 3, and finally section 4 includes discussion, conclusion and proposed future work.

II. FINGERPRINT SENSING

In our developed system we used a chip (FPS110) manufactured by Veridicom Company [7]. The advantage of using the solid-state capacitance fingerprint sensor (chip) is its low cost, compact, rigid, small size 1"(width) X 1"(height) X 0.102" (depth), ultra-hard protective and chemical resistant coating makes it the best current scanner for fingerprint image sensing and is likely to be embedded in a number of devices such as cellular phones and laptop computers [2]. We wrote the software that can communicate with the chip and capture the fingerprint images into our program that pre-process, extract features, post-process, and match fingerprint images. Any fingerprint (biometrics) based verification system consists of the following parts (Fig. 4): (i) User interface, (ii) System database, (iii) Enrollment module and (iv) Authentication. In the enrollment module, the user is asked to put his fingertip on the fingerprint sensor then the system retrieves a PIN (Personal Identification Number) for the user by which the user will authenticate himself each time. In the authentication module the user is asked to enter his PIN then putting his fingertip on the sensor. In both modules the fingerprint sensing is a crucial step. The user interface is just for controlling the user interaction with the biometrics (fingerprint) verification system. The system database is holding the IDs, fingerprint features and personal information for whom it is allowed to use the attendance system or access the protected data. The authentication module is responsible for the decision with true match or fraud.

In addition to the mentioned advantages, this sensor containing a built-in flash ADC that automatically converts the analog capacitance values, which represent the touch

strength on the sensor surface, to a digital 8-bit raster pixel values, which can be read directly by a digital microcomputer.

The last and most important advantage for the capacitance solid-state chip over the pre-mentioned ones is its capability to produce high quality images over different conditions of dryness, wet and dirty. This can be implemented by changing the current and the time values

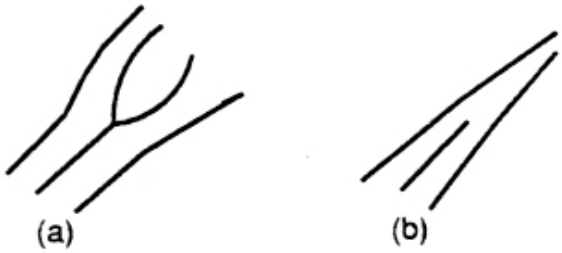

Fig. 1. Two commonly used fingerprint features (a) Ridge bifurcation; (b) Ridge ending

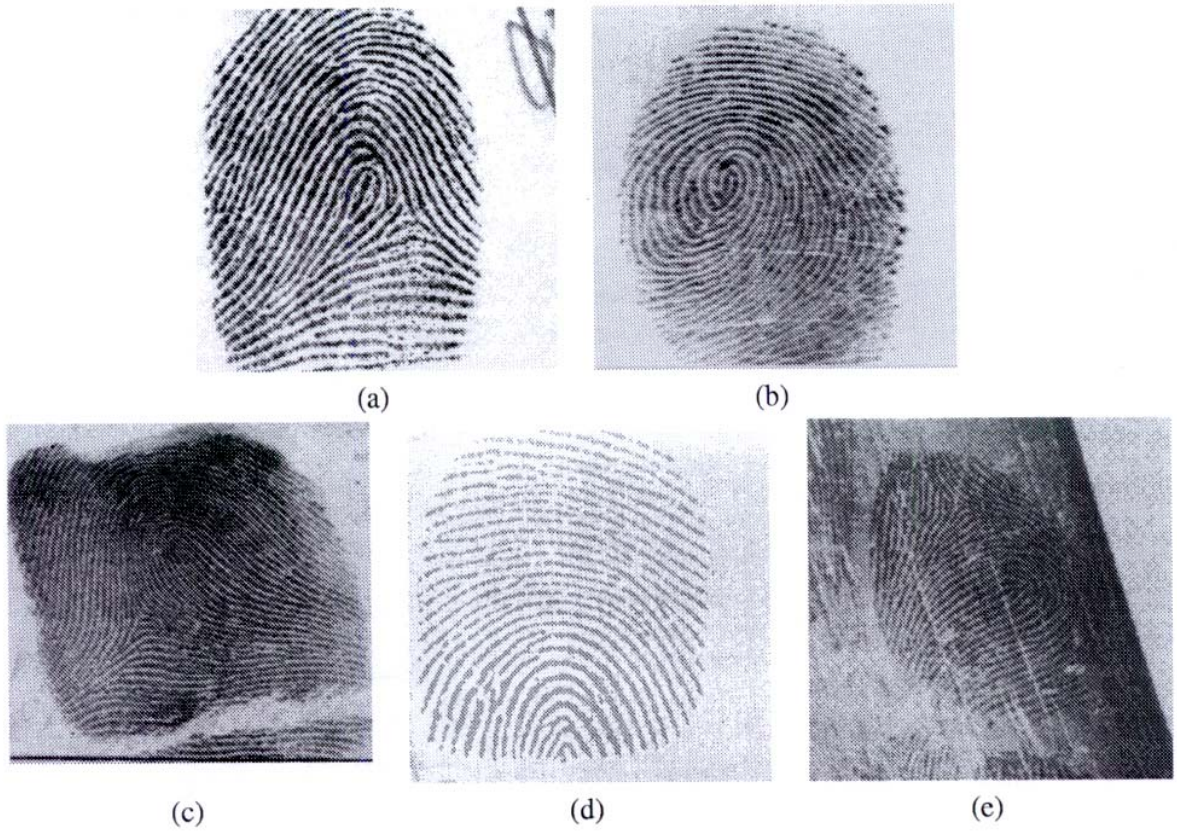

Fig. 2. Fingerprint sensing: (a) An inked fingerprint image could be captured from the inked impression of a finger; (b) a live scan fingerprint is directly imaged from a live finger based on optical total internal reflection principle: the light scatters where finger (e.g., ridges) touch the glass prism and light reflects where finger (e.g. valleys) does not touch the glass prism. (c) Rolled fingerprints are images depicting nail-to-nail area of a finger. (d) Fingerprints captured using our solid-state sensor show a smaller area of finger than a typical fingerprint dab captured using optical scanners. (e) A latent fingerprint refers to partial print typically lifted from a scene of crime.

needed for fingerprint scanning and included in an Automatic Gain Control (AGC) software module to adjust pixel or row or local area as given by eqn. (1):

$$I = C*(dv/dt) = C*(V1-V2)/\Delta t \quad (1)$$

Where: I is the constant capacitor discharge current (can be set by an internal register in the fps110 sensor), C capacitance value, V1 the initial capacitance voltage (constant and equals Vcc at the start), V2 final capacitance value (the output pixel) and Δt is the time from V1 to V2 (can be set by an internal register in the Veridicom chip). Using an ISA prototype card that provides 1-2 Mbytes/Second data transfer rate, we interfaced the capacitance fingerprint chip fps110 (Trademark of Veridicom, Inc.) to the IBM compatible PC data bus, see the interfacing module block diagram in Fig. 3. The resultant total fingerprint image scanning time was nearly 1 Sec., which is acceptable for the on-line fingerprint verification; Fig. 5 (left) shows an image acquired using our sensor.

III. FINGERPRINT VERIFICATION

After the fingerprint image was scanned and loaded in the microcomputer RAMs, the following steps are followed in order to purify and extract the input fingerprint features for either registering it as a template in the system database or matching it with an existing template:

1) Coherence enhancement using nonlinear diffusion

Because the quality of the acquired images isn't assured to be well an enhancement process must run on the image to increase its quality [3].

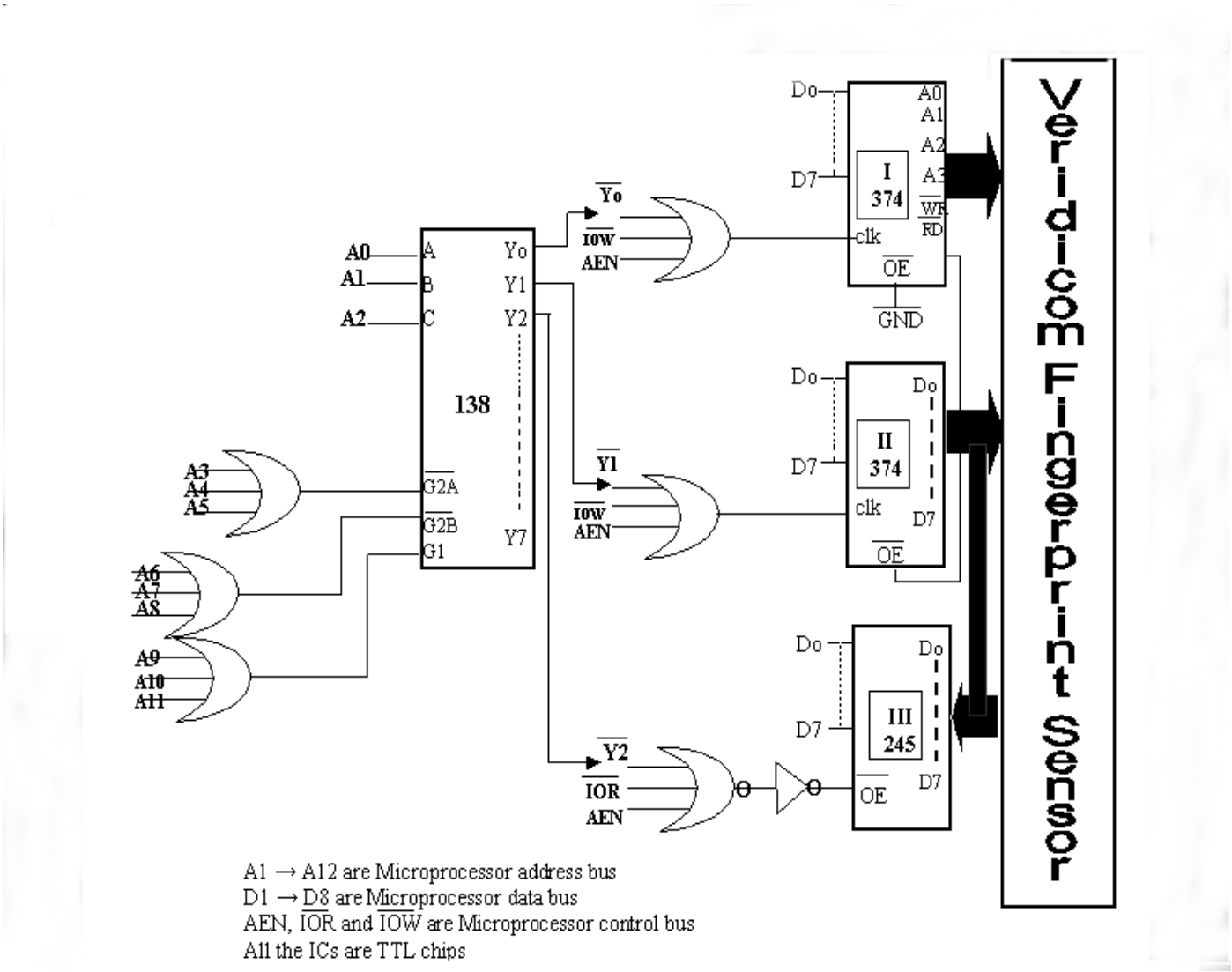

Fig. 3. Interfacing Module Block Diagram

The solution of the diffusion equation (2):

$$It = div(c(x,y,t)\partial I) = c(x,y,t).\Delta I + \partial c.\partial I \quad (2)$$

was included in appendix 1. We involved the pixels 8-neighbors in gradient computation instead of 4-neighbors. An example for fingerprint image after 3 iterations of the diffusion algorithm is shown in Fig. 5 (right).

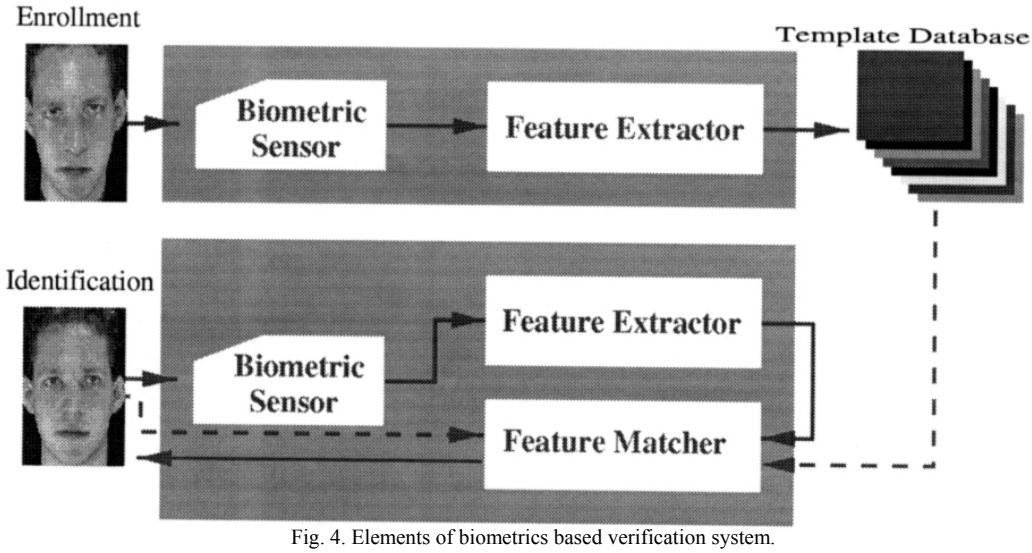

Fig. 4. Elements of biometrics based verification system.

2) Binarization (Thresholding)

This stage aims to differentiate between the ridge points (set to black) and the furrow (valley) points (set to white) due to the unequal pressure of the finger on the sensor surface the global threshold fails; we used the Region Average Threshold (RAT) because it segments the image pixel corresponding to 7X7 region of its neighbors. We used the standard deviation to differentiate between the background areas and the finger regions; Fig. 6 shows a segmented fingerprint image.

Fig. 5. An image acquired using our sensor (left), Diffused fingerprint image itr. = 3, λ = 0.125, neighborhood = 8 (right).

3) Binary Image Thinning

We used the thinning algorithm proposed in [4] due its computational simplicity, fast, efficiency and does not affect the singular points, Fig. 7 shows a thinned fingerprint image.

4) Feature extraction and post-processing

The thinned image is ready now for extracting the singular points (the points needed for fingerprint recognition) e.g. terminations, bifurcations, its directions and the number of ridges crosses the line between the minutiae. Due to the low quality of acquired image, local distortion and the image enhancement module itself may lead to a false minutiae, post-processing stage that increases the percentage of true minutiae compared with the false ones is essential [5]. Fig. 8 shows feature extraction process before post-processing while Fig. 9 highlights the post-processing false minutiae detection.

5) Parameterized point matching algorithm

The algorithm proposed in [6] was used, it considers: the feature type (termination or bifurcation), translation, rotation, local distortion to match the live scanned fingerprint image against the enrolled one in the template data base to result: Match or No-match.

Fig. 6. Segmented fingerprint image.

Fig. 7. Thinned fingerprint image.

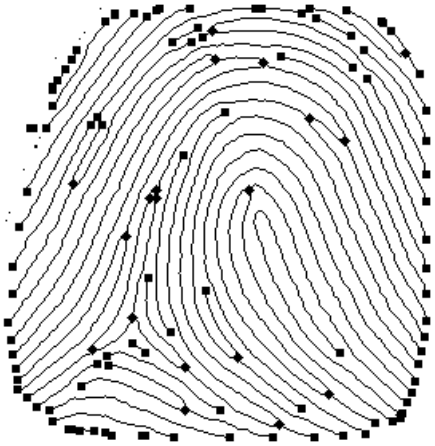

Fig. 8. Feature Extraction before post-processing.

Fig. 9. Feature Extraction after post-processing.

IV. CONCLUSION AND FUTURE WORK

The aspects of the automatic fingerprint authentication system discussed was implemented in Cairo University, School of Engineering, systems and biomedical dept. and the software module was implemented using VC++ (Trademark of Microsoft Corp.). We acquired 100 subjects (pairs) and we could verify this small number and we had efficiency over 99.8%. In future we will calculate the FAR and FRR for a larger dataset (10000). The price for the overall verification system will be less than 1000$ for commercial production. The system can be applied at doors lock, banks for verifying identity, airports, attendance systems and ATM (automatic teller machines).

V. APPENDIX I

The diffusion algorithm function on a 3x3 window, calculate the gradients (4 neighbors or 8 neighbors) and update the center pixel of the window every iteration according to equation (3):

$$I(i,j)|t+1 = I(I,j)|t + \lambda [(Cn.\partial n\ I) + (Cs.\partial s\ I) + (Ce.\partial e\ I) + (Cw.\partial w\ I)]|t \quad (3)$$

Where $\lambda = 1/4$ for 4 neighbors or 1/8 for 8 neighbors, and the symbol ∂ indicates nearest neighbors' differences:

$$\partial n\ I(i,j) = I(i-1,j) - I(i,j)$$
$$\partial s\ I(i,j) = I(i+1,j) - I(i,j)$$
$$\partial e\ I(i,j) = I(i,j+1) - I(i,j)$$
$$\partial w\ I(i,j) = I(i,j-1) - I(i,j)$$

The conduction coefficient is updated at every iteration as a function of the brightness gradient:

$$Cn = g(|\partial I(i+0.5,j)|)$$
$$Cs = g(|\partial I(i-0.5,j)|)$$
$$Ce = g(|\partial I(i,j+0.5)|)$$
$$Cw = g(|\partial I(i,j-0.5)|)$$

The choice for the g(.) is as follows:

$$g(x)=\exp.((-X/K)^2)$$

Where K is taken to be the 90 percentile of the image histogram at every iteration, X is the ∂I.

VI. REFERENCES

[1] M. Abu Elnaga," *The science of applied fingerprints* ", [in Arabic], 1984.

[2] A. K. Jain, R. Bolle and S. Pankanti (eds.). *Biometrics: Personal Identification in Networked Society*. Kluwer, New York, 1998.

[3] P. Perona and J. Malik," Scale Space And Edge Detection Using Anisotropic Diffusion," IEEE Transaction Pattern Analysis and Machine Intelligence, vol. 12, No. 7, PP. 629-639, July 1990.

[4] B. K. Jang and R. T. Chin," One-Pass Parallel Thinning: Analysis, Properties, and Quantitative Evaluation," IEEE Transaction Pattern Analysis and Machine Intelligence, vol. 14, No. 11, PP. 1129-1140, Nov. 1992.

[5] Q.Xiao, H. Raafat," *Fingerprint image postprocessing: A combined Statistical and structural approach*," Pattern Recognition, vol. 24,no. 10,pp. 985-992,1991.

[6] Shin-hsu Chang, Fang-hsuan Cheng, Wen-hsing Hsu, and Guo-zua Wu, "*Fast algorithm for point pattern matching: Invariant to Translations, Rotations, and Scale changes*," Pattern Recognition, Vol. 30, No. 2, pp. 311-320, 1997.

[7] www.veridicom.com.