

A Full Fingerprint Verification System for an Integrated Single-line Sweep sensor

Nicolas Galy, benoît Charlot and Bernard Courtois

Abstract— This paper presents a full fingerprint verification system. It is composed of a tactile fingerprint sensor, integrated read out and conversion circuits, and dedicated recognition algorithms. The sensor is a single line sweep mode sensor, e.g. it is made of single line of sensing elements, thus covering the minimum surface of silicon. Compared to cm^2 sized touch sensors, it offers a large cost reduction and possibility of easy integration into portable devices. The use of a single line to measure fingerprint requires the user to sweep its finger along the sensor. This sensing scheme produces fingerprint images with several distortions that needs further image processing to allow efficient fingerprint recognition. This is why we developed and present here specific algorithms to take care of the sensor's specifications. The paper will present measurement results as well as a performance evaluation of the entire verification system.

Index Terms— Fingerprint Verification, MEMS, Cantilever, CMOS, bulk micromachining, Sweep Sensor, Tactile sensor, Enhancement, Distortion, Performance Evaluation.

I. INTRODUCTION

Biometrics[1] is the extraction of physical or behavioral parameters peculiar to a person with the aim of identification in a reliable way. Several personal biological characteristics are now used in biometric systems; it is for example iris, fingerprint, voice or face. These biological characteristics are unique and thus more reliable to identify people than traditional methods based on features that we have (key, card) or we know (password). Biometrics is now appearing in several part of our everyday life such as building access, and computer login. Within all biometric techniques, digital fingerprint recognition is the most widely used for personal identification with quite the half of the total biometric market [2]. It is no longer associated only with police and has been accepted by a large part of the population as a fast, secure and easy way of personal identification.

A fingerprint is a set of ridges and furrows with singular points, mainly ridge ending and bifurcation, called minutiae (Fig. 1). This pattern is universal, permanent and unique for each person [3].

Usually, acquisition of a fingertip image has been made with the use of ink and paper. Optical devices were created in order to automate this task. Most of these optical sensors

are made with a CCD sensor and prismatic optics. They are mainly used for building access control and remain costly and bulky for any other application. Thanks to the emergence of low cost integrated devices, biometric

identification that was previously reserved for security applications is now reaching several other applications. Integrated fingerprint sensors have become indeed a mass-market application, and nowadays we can find such devices in cell phones and laptop computers.

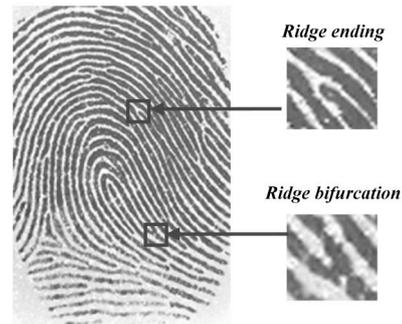


Fig. 1. Example of minutiae from a fingerprint.

Most integrated fingerprint sensors have been developed with microelectronic silicon technologies. Several measurement techniques have been developed so far for the capture of fingerprint [4]. The most employed is the capacitive technique [5]-[9] where the device senses the electrical capacitance between the skin (ridges in contact or valleys) and a reference electrode on the surface of the sensor. Other techniques such as thermal [10]-[11], pyroelectric materials, optical [12]-[13] or mechanical [14]-[15] transduction mechanisms have also shown great potentials and successful results.

Among different fingerprint sensors, we see three kinds of acquisition mode as depicted in Fig. 2. Full matrix sensors, also called touch sensors, are the most common type. It requires the user to press his finger on top of the sensor surface for the capture. The image is available instantaneously and without spatial distortion except misalignments and rotations. The drawback is the large required surface ($>1\text{cm}^2$), which leads to costly sensors. In order to overcome this problem, sweep sensors have been developed [17]. Users have then to sweep their finger along the sensor. Most of them use a partial matrix that contains a reduced number of lines (typically from 8 to 40). The fingerprint image is then reconstructed by overlapping a set of partial images, which enables to remove distortion produced by the finger speed non-uniformity. Finally, single row sensors offer the lowest silicon surface, but fingerprint images may contain a great distortion with areas of different sweeping speed. This effect may reduce significantly the recognition performance of the system; this is the reason why dedicated algorithms have to be developed specifically for this latter type of sensors.

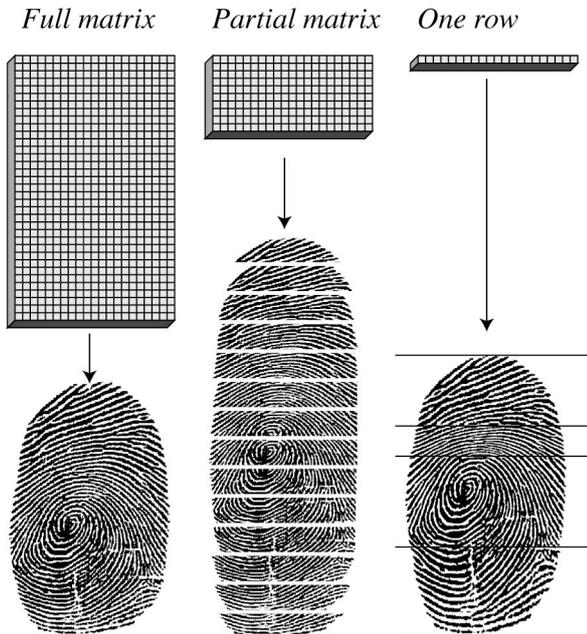


Fig. 2. Schematic of the measurement principle of the full matrix (left), partial matrix (center) and one row (right) fingerprint sensors and their relative output: the full scale image, the superposed images and the distorted image.

In this paper, we detail a full fingerprint verification system for a single user application. The system has to confirm or deny a person's identity compared with a reference record ("Am I who I claim to be?"). The fingerprint verification system has been entirely developed in our laboratory and is composed of a digital integrated sensor and a programmable microcontroller that drives the sensor and records data. Specific fingerprint recognition algorithms are then processed for the moment with a computer but will be soon integrated into the microcontroller in order to have a stand-alone system. The paper will begin in section II with a description of the acquisition system and general features of the sensor. A focus will be made on the particularities of images produced by the sensor. Then the paper will detail the entire recognition and verification process. The pre-processing step, which enables to enhance the quality of the fingerprint image is discussed in section III while section IV will report signature extraction which is based on minutiae features. Verification process that consists in matching the signature with the recorded one is described in section V. Finally, System performance evaluation is analyzed in section VI by means of both synthetic and real fingerprint databases.

II. ACQUISITION

Acquisition enables to get an image from the user's fingerprint and is the first step of a verification system. In this section we describe main features of the acquisition system and of the images produced by the sensor.

A. The sensor

The sensor, as depicted in Fig. 3, has two main features with respect to standard industrial solutions: it is a sweep sensor and it is a tactile, e.g. mechanical sensor. The sensor is build from an integrated bulk micromachining technology. So it combines both MEMS and electronics in the same substrate. As can be seen in Fig.3, three rows of 256 cantilevers are

implemented in the sensor, however only one is actually used for measurement. It is possible to switch from one line to another. It has been made to further use several lines as a partial matrix sensor. Dimensions of the sensor are 1.6x16mm. The spatial resolution is 508 dots per inch, which gives from 5 to 10 points between two ridges.

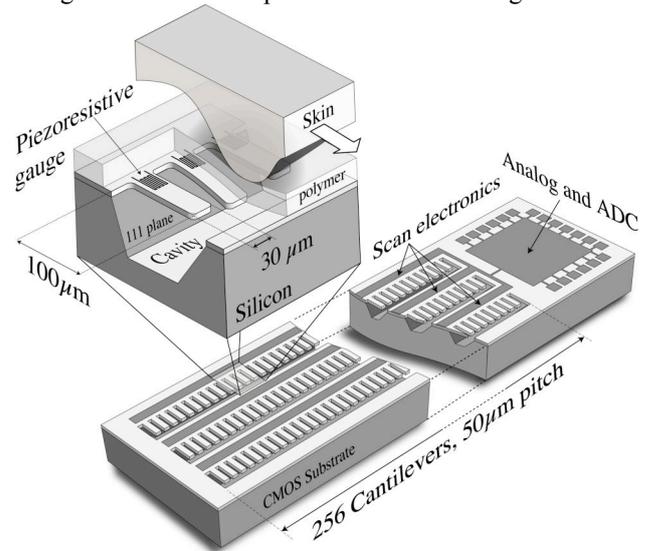


Fig. 3 Schematic of the fingerprint sensor with piezoresistive cantilevers. A polymer protective sheet protects the sensor against abrasion and corrosion.

In order to obtain a fingerprint image, the user has to sweep its finger on the surface of the sensor, perpendicularly to the chip. During this, the sensor scans the cantilevers line and measures the movement of cantilevers sequentially. The electronics and connection pads, placed on one side of the chip are protected by resin (see Fig.4). Since human skin could be strongly corrosive for electronics, a protective polymer sheet is laid on the surface of the sensor. Several materials have been tested and the best results were obtained with a 12µm polypropylene sheet. It has enough strength to protect the sensor and low stiffness to avoid blurring the mechanical signal.

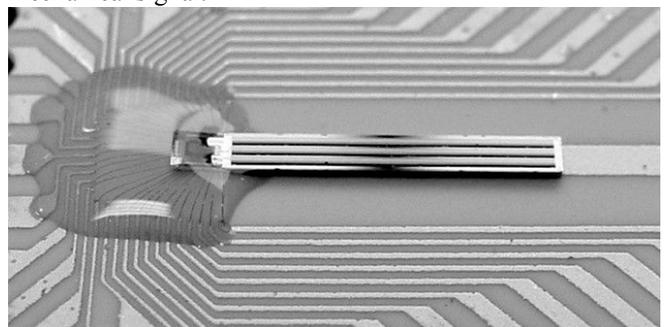


Fig. 4 Photo of the fingerprint mounted on a ceramic printed circuit board. A droplet of resin protects wirebonds.

B. Fabrication process

The sensor is made by means of a CMOS-compatible front-side bulk micromachining technology (FSBM). The CMOS is an Austriamicrosystems 0.6 µm triple metal process obtained via the Circuit-Multi-Projects[16] multi project wafer service. The FSBM technique consists in designing openings through the different CMOS layers so as to obtain naked silicon areas on the surface. The passivation (Silicon Nitride) layer acts as a mask for the post process etching. After the fabrication of the microelectronic layers, a

TMAH anisotropic wet etching post-process allows suspending microstructures by attacking the silicon with respect to the passivation where creating a cavity (see Figure 3 and 5) on the silicon substrate. This technique is operated at chip level without the need of any additional lithographic process.

Cantilevers are then composed of a sandwich of all the layers present in the CMOS technology: isolation oxide, gate oxide, polysilicon of the grid, deposited interlevel oxides, interconnection metallic layers and finally silicon nitride passivation layer. The total thickness is around 4 μm .

This stable low cost MEMS technology allows integrating the sensor part and electronic circuits in the same chip. Figure 6 shows SEM micrograph of the chip after TMAH release of the cantilevers.

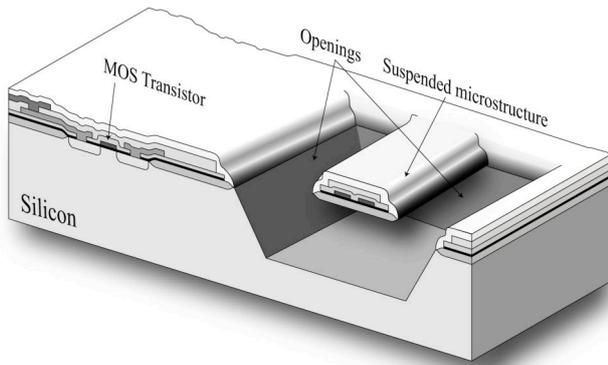


Fig. 5 Cross section schematic of the CMOS compatible front side bulk micromachining technology employed for the fingerprint sensor.

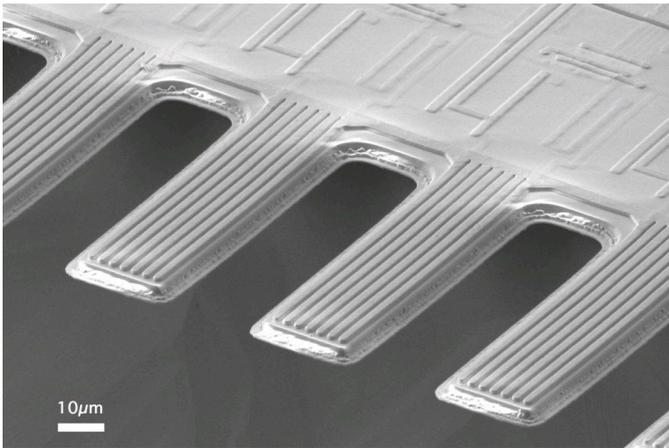


Fig. 6 Scanning electron microscope image of the cantilevers.

C. Piezoresistive measurement

The tactile measurement is based on the use of micro cantilever embedding a piezoresistive strain gauge (See Fig.3 and Fig.5). The cantilevers are made of a stack of insulating layers (SiO_2 and Si_3N_4) and contain polysilicon and metal lines. The skin, swept along the sensor, induces downward deflection of cantilevers when it is in contact with the sensor's surface. When there is no local contact, the case of a ridge, cantilevers remain flat. This tactile scheme works because cantilevers are small compared to a finger's ridge period and because the skin, thanks to its elasticity, penetrates a little in the cantilever's cavity. The bending of cantilevers induces a stress distribution in the material. The piezoresistive gauge made of polysilicon (the material used

for the grids of transistors) is placed near the clamping of the cantilever. Its resistivity changes regarding the stress level in the material, through the longitudinal and transverse piezoresistive coefficients (Table 1). As the gauge is placed in the lower part of the cantilever's thickness, below the neutral fiber plane, it is compressed when the cantilever bends downward. Within the maximum displacement, the resistance variation reaches 6%. Table 1 summarizes cantilevers parameters.

TABLE I
CANTILEVERS PARAMETERS

<i>Microbeam parameters</i>	<i>value</i>
Length	100 μm
Widths	30 μm
Thickness	$\sim 4\mu\text{m}$
Pitch	50 μm
Out of plane stiffness (computed)	186 Nm^{-1}
In plane Stiffness (computed)	10075 Nm^{-1}
Sensitivity	171 – 295 N^{-1}
Natural frequency	690 kHz
Width of the micromachined cavity	210 μm
<i>Polysilicon gauge parameters</i>	<i>value</i>
Width	1.2 μm
Length	8x28 μm
Nominal resistance	6.5 $\text{k}\Omega$
Nominal resistance mismatch	1.73%
Longitudinal piezoresistive coefficient	$-1.3 \cdot 10^{-10} \text{ Pa}^{-1}$
Transverse piezoresistive coefficient	$7.6 \cdot 10^{-11} \text{ Pa}^{-1}$

D. Read out integrated circuit

The sensor embeds a read out integrated circuit (ROIC) that performs three main tasks: Scanning of the cantilever row, measure and amplification, and conversion to a digital signal. The sensor has digital input and output, its can be drive by a digital microcontroller. A photo of the chips is presented in Fig. 8 and schematic of the ROIC in Fig.7. Whole chip contains about 53,000 transistors

The measurement of the stress gauge is made with a switch capacitor architecture in order to have an offset cancelling circuit, thus avoiding the use of a calibration step during operation.

The sequential measurement of cantilevers is controlled by a shift-register composed of D flip-flop cells driven by a clock signal from 20 to 200 kHz. The gauge resistance circuit uses a correlated double sampling switch capacitor architecture driven by a pair of non-overlapping clocks (ϕ_1 and ϕ_2). This architecture makes possible to cancel the DC offset caused by the op-amps and at the same time reduces low frequency noise. The pixel electronic allows performing a differential measurement between the gauge and a reference resistor placed above the bulk silicon where the mechanical strains are nonexistent. The gauge resistance change is transformed into a current signal and feeds a transresistance amplifier through the transmission line that is biased at a constant voltage. In this way it is possible to get rid of parasitic capacitance of this very long analog interconnect line (in the case of the first pixel, this line has a length of about 1.28 cm).

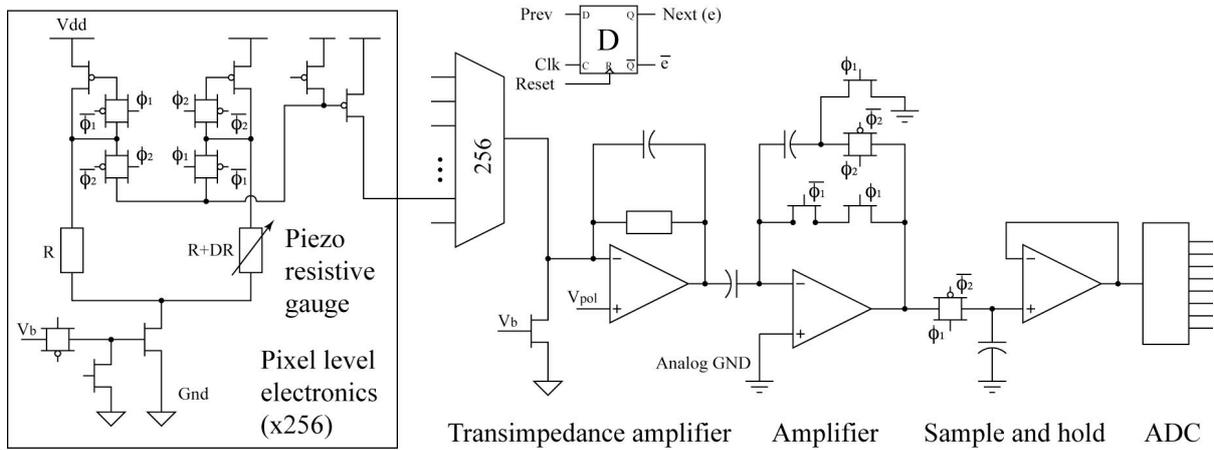


Fig. 7. Schematic of the Read Out Integrated Circuit.

The analog signal is digitalized using an 8 bit converter so as to provide the value of the gauge resistance change by the way of a digital parallel bus. The implemented A/D converter uses successive-approximation architecture. It employs a simple folded resistor ladder. The comparator is based on offset cancellation switch capacitor architecture. The ADC can work up to 1 MSamples/s with a precision of 7.7 effective bits. A detailed description of the internal circuits of the sensor is given in [18].

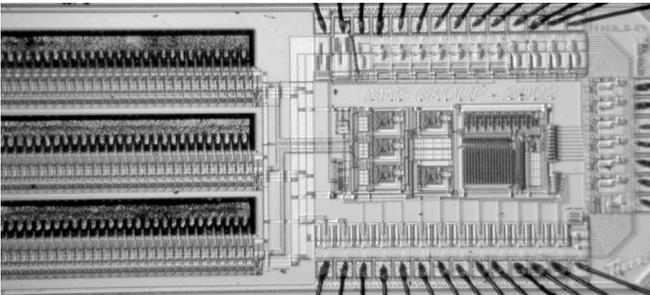


Fig. 8. Photo of the chip showing the electronic circuits on the right and the beginning of the cantilevers line on the left.

E. The acquisition driver

The sensor chip is driven by means of a connection to an APEX development board from Altera [19], which executes the acquisition program. This board includes a 32bits NIOS processor placed on a FPGA circuit with 256kB of memory and is parameterized by means of a hardware configuration file that provides a great flexibility of use. The sensor and the board interact by means of four digital signals:

- RESET initializes the sensor at the starting.
- CLOCK specifies cantilever scan frequency and is also - used to feed the switch capacitor circuits.
- LAST indicates the end of a row.
- DATA corresponds to the byte value of the cantilever that has been read.

The board is linked to a computer in order to load the driver and to retrieve images. A picture of the system is represented on Fig. 9.

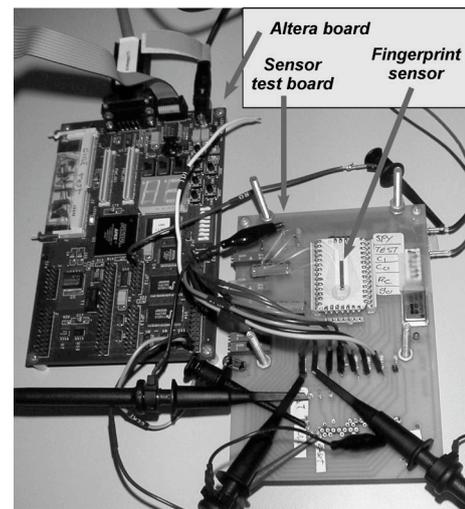


Fig. 9. Photo of the experimental platform which enables image acquisition.

As the sensor works continuously, the output is composed of series of 256 bytes representing the scan of one row. These series of lines may form a rectangular image with an infinite height. So a specific program has been implemented in order to detect both starting and ending of the finger contact. By computing the sum of each line, we can detect the presence of a finger on the sensor. The difference between the presence and the absence of the finger is large thanks to the sensitivity of the cantilevers and the amplification circuit. So we have set a specific threshold in the 256 possible values that defines the beginning and the ending of the fingerprint scan (see Fig. 10).

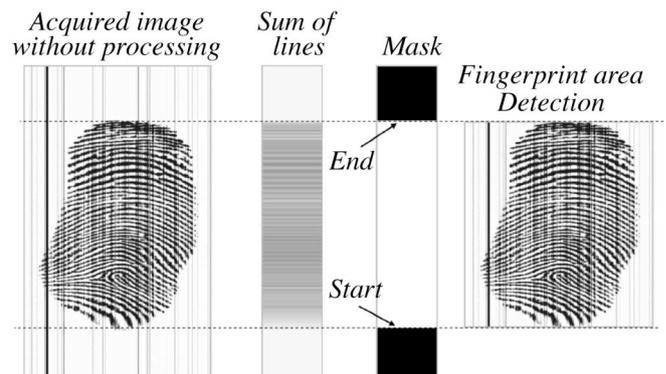


Fig. 10. Detection of the fingerprint area during finger sweep.

After each acquisition, the image is stored on a computer in order to visualize it on screen and to create a database of measured fingerprints for tests. This database is available for downloading in our server [20]. The cantilever scanning frequency was set to 100kHz; this means that the acquisition lasts about one second for a 256x390 image. After a training phase this turned out to be enough for most users. Indeed as shown on Fig. 11 the image height H varies roughly between 200 and 400 pixels.

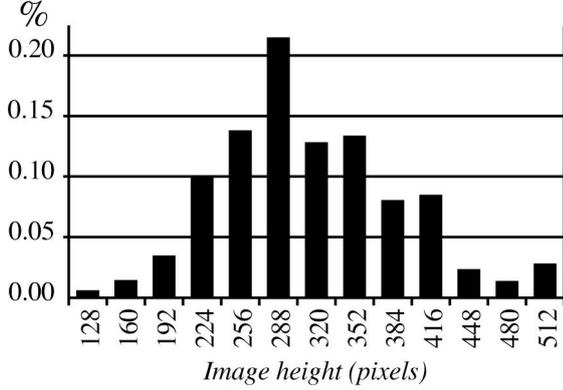


Fig. 11. Histogram of the image height from the fingerprint database.

F. Main features of fingerprint images obtained with the sensor

Fig. 12 shows an example of an image generated by the sensor. Because of the sweep mode we have a variable height H whereas the width W remains constant at 256 pixels (i.e. the number of cantilevers). When analyzing the grey levels histogram we can notice the high contrast of the image. We have mainly a binary image: background is white whereas ridges are black with little shade. This observation implies that the user presses his finger on the sensor with a sufficient pressure. By looking at the background of the image we can highlight some particularities. First, we note the presence of vertical black lines. The reason of these black lines is the fracture of cantilevers. The latter are relatively weak and may break when an excessive or a non-vertical pressure overloads them. A broken cantilever does not transmit electronic signal any more and behaves like a "dead pixel" (black point). Due to the sweep mode this will cause the presence of a vertical black line in the resulting image. If we watch the background more precisely we also see light grey vertical dotted line (as if some cantilevers slightly shake). This problem is currently still under consideration and seems to have an origin in the analog amplification chain.

Inter-ridge spacing is roughly constant in a fingerprint. This assumption is verified for images originating from touch sensors. As we have a single-row pixel sensor without image reconstruction algorithm, speed non-uniformity during acquisition may generate a large inter-ridge distance variation (e.g. we can distinguish roughly 3 areas with distinct speed on Fig. 12). As the finger is moved vertically the distortion is small where ridges are vertical, whereas the sweeping mode effect may be considerable anywhere else.

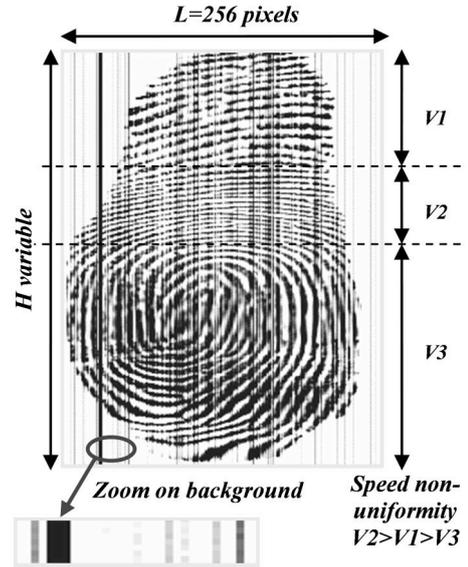


Fig. 12. Main features of raw images produced by the sensor.

According to our observations and by assuming a trained and cooperative user we considered an inter ridge distance range (2) where ridge direction θ is roughly vertical, and (1) elsewhere.

$$|\cos\theta| > \cos(\pi/8) \Rightarrow \Delta d = [3..15] \text{ pixels } [\Delta B = 2.3 \text{ octave}] \quad (1)$$

$$|\cos\theta| \leq \cos(\pi/8) \Rightarrow \Delta d = [6..12] \text{ pixels } [\Delta B = 1 \text{ octave}] \quad (2)$$

III. PRE-PROCESSING

Once the fingerprint has been acquired, a *pre-processing* step is needed in order to enhance image quality. To do so we take benefit of particularities of fingerprint images and use a frequency domain filter.

A. Segmentation

The first step of the pre-processing is the segmentation of the image. The goal is to separate the foreground from the background [21]. The foreground corresponds to the fingerprint area in contact with the sensor during the acquisition. The background represents the noisy part around the fingerprint and contains no useful information. We have seen in section II that images have a very high contrast, this is the reason why we decided to use the mean grey value as segmentation feature.

The image is first divided into non-overlapping blocks of 16x16 pixels and the average grey value of each block is computed. If the latter is below a threshold T , then we consider the block belongs to background. As the grey values vary in the range [0..255] and as images are highly contrasted, we used $T=128$. An additional operation is performed on the mask in order to delete noisy areas: blocks with at least 3 neighbors labeled as background and blocks at the edges of the image are associated with the background. The complete operation is illustrated on Fig. 13. The background is not processed in the subsequent operations; this enables a gain of calculation time and a more reliable feature extraction.

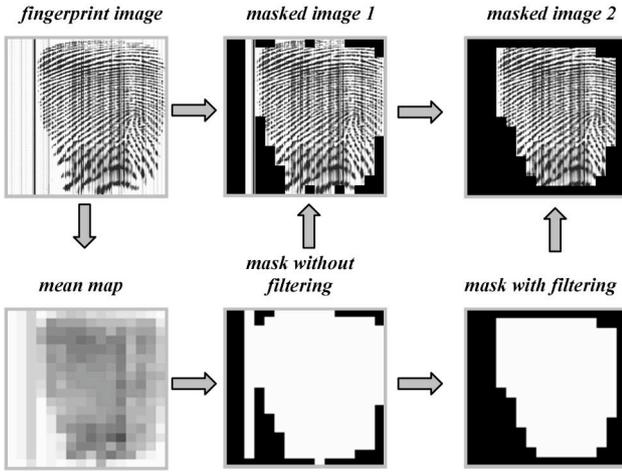


Fig. 13. Example of segmentation on a fingerprint image.

B. Enhancement

To improve fingerprint image quality, filters extensively exploit local features [22], i.e. the local ridge direction and frequency.

1) Log-Gabor masks

It is generally accepted that the average inter-ridge distance f_0 does not vary much in a fingerprint, and Gabor filters are widely used because they have optimal resolution in both spatial and frequency domains ([23]-[26]). f_0 is then determined statistically by taking an average value [24]. Nonetheless there may be slight variations due to the skin elasticity or between two distinct persons for a given population. In this case f_0 is estimated locally to tune the filter [26]. In both cases the inter ridge distance is considered locally constant and the bandwidth of the filter does not exceed 1 octave. As regards our sweep sensor this assumption is false as the speed can change in course of the acquisition according to the user's behaviour (see II). Here we need to extract broad spectral information such as $\Delta B=2.3$ octave (1). Unfortunately the maximum bandwidth of Gabor filters is limited to roughly one octave [27], this is the reason why we decided to use oriented Log-Gabor filters. The latter are defined in the frequency domain by the product of a radial component and an angular component:

$$H(f, \theta) = H_r(f) \times H_\theta(\theta) \quad (3)$$

The radial component is a Gaussian function viewed on a logarithmic scale (4) where f_0 is the tuning frequency, and σ_r determines the radial bandwidth of the filter.

$$H_r(f) = \exp \left\{ - \frac{[\ln(f/f_0)]^2}{2[\ln(\sigma_r/f_0)]^2} \right\} \quad (4)$$

The transfer function of the angular component is given by (5) where θ_0 represents the direction of the filter, and σ_θ determines the angular bandwidth of the filter.

$$H_\theta(\theta) = \exp \left\{ - (\theta - \theta_0)^2 / 2\sigma_\theta^2 \right\} \quad (5)$$



Fig. 14. Representation of radial (a), angular (b) and full mask components from the Log-Gabor function.

If one compares them to Gabor filters, they allow arbitrarily broad bandwidth and they have always a zero DC component, they are thus a good alternative [27].

The radial bandwidth of the Log-Gabor function is defined by $\Delta B = \log_2(f_{\max}/f_{\min})$ where f_{\max} and f_{\min} are the solutions of $H_r(f)=1/2$. We get:

$$\Delta B = 2\sqrt{2/\ln 2} \times |\ln(\sigma_r/f_0)| \quad (6)$$

$$f_0 = 2^{\frac{\Delta B}{2}} \cdot f_{\max} \quad (7)$$

By computing the angular bandwidth we get similarly:

$$\Delta \Omega = 2\sigma_\theta \sqrt{2 \ln 2} \quad (8)$$

By using $\Delta \Omega = \pi/8$ and equations (1) and (2) according to the filter orientation, we get a bank of 8 oriented Log-Gabor masks. Assumption (2) is used to compute the horizontally oriented mask and enables to limit the vertical black lines effect observed in II. These masks are computed offline and are stored in the memory of the system.

2) Masking

The image is first divided into blocks of $W \times W$ pixels. Then the Fast Fourier Transform (FFT) of each block is computed and the local features of ridges inside the block (i.e. the direction and the frequency) are estimated. The direction enables to choose the corresponding mask whereas the frequency will be used in the matching step (see section V). Finally the block is masked with its associated oriented Log-Gabor filter, and the inverse FFT is computed to get the corresponding enhanced block. These operations are executed for all blocks from the foreground image and are illustrated on the next figure.

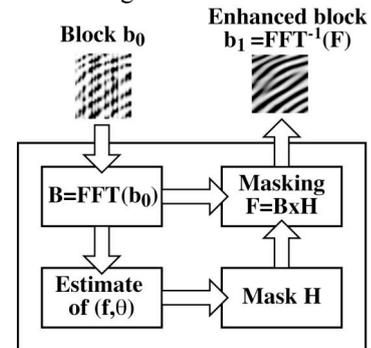


Fig. 15. Principle of directional masking.

W has to be a power of 2 in order to implement a fast computation of the FFT, furthermore overlapping blocks have to be used to avoid edge effects between adjacent blocks. We defined experimentally blocks of 32×32 pixels with an overlap of 24 pixels.

IV. FEATURE EXTRACTION

The fingerprint enhancement is followed by the *signature extraction*, which extracts the useful fingerprint properties for recognition. Most fingerprint verification systems use minutiae information and extensive researches have already been made in this field [28]. To extract the minutiae features, we have implemented the common approach, which consists in using a thinned representation of the enhanced fingerprint image.

A. Binarisation and thinning

The fingerprint image has to be binarized prior to the

thinning. As the Log-Gabor masks have a zero DC component, each filtered block has a null mean value. So we easily obtain a binary image by comparing each resulting pixel with zero. This can be done by applying the threshold directly at the output of the filtering step by means of a simple comparator. This enables a gain in time (a new image sweep is not needed to perform binarization), and a gain of memory (a binary digit is stored instead of a floating point number).

Then the resulting binary image is thinned by means of a succession of morphological erosion operations. To do this task we used the Rosenfeld's algorithm [29] due to its simplicity, but numerous other approaches exist [30]. With a view to a possible hardware implementation this choice will have to be reviewed as it can reduce significantly the calculation time [31]. An example of the different steps leading to a skeletonized fingerprint is illustrated on Fig 13.

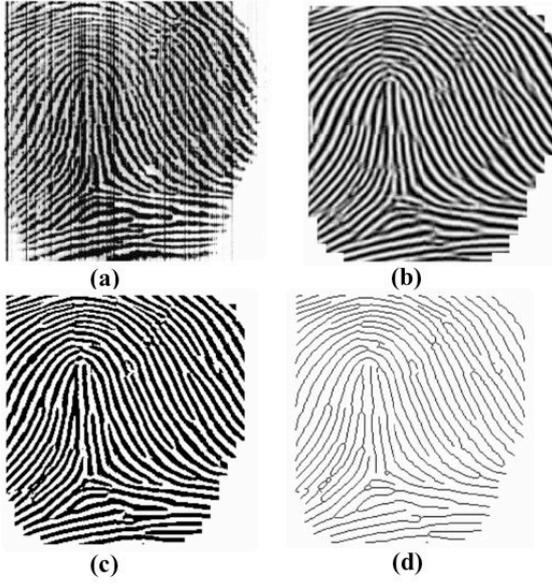


Fig. 16. Illustration of the different steps of thinning on a sample fingerprint record from the sensor: acquired image (a), filtered image (b), binarized image (c) and thinned image (d).

B. The signature file

Once we have a skeleton of the fingerprint image it becomes very easy to detect minutiae by means of the Crossing Number (CN):

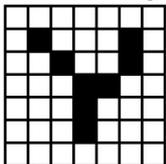
$$CN(P) = \frac{1}{2} \sum_{i=1}^8 |P_i - P_{i-1}| \text{ with } P_8 = P_0 \text{ and } P_i \in \{0,1\} \quad (9)$$

$CN(P)$ represents the number of ridges coming from the pixel P . It is computed for each black pixel (Fig. 17) and two values are considered:

$CN(P)=1$: P is a ridge ending

$CN(P)=3$: P is a bifurcation

Representation of the skeletonized image



Binary coding

0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	0
0	0	1	0	0	1	0	0	0	0
0	0	0	1	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0

CN coding

0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	1
0	0	2	0	0	2	0	0	0	2
0	0	0	3	2	0	0	0	0	0
0	0	0	2	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0

Fig. 17. Example of Crossing Number coding from the binary representation.

Although simple this method causes the detection of numerous false minutiae as we can see on Fig. 18. More than hundred minutiae are detected while a fingerprint has roughly less than 100 true minutiae. An additional processing is thus necessary to remove the false information. To do this task we use empirical rules by considering that two true minutiae are seldom nearby in practice. We have applied the two following rules to the detected minutiae in order to eliminate quickly the maximum of false minutiae:

- Minutiae at the boundary between the fingerprint and the background are deleted.
- Two minutiae which are on the same ridge and whose distance is less than a defined threshold are removed.

Other additional techniques have been proposed in literature ([32]-[34]) at the expense of a longer computation time. This has nonetheless proved to be enough in our case with roughly less than one hundred remaining minutiae after the cleaning step.

For each validated minutiae M_i we extract 3 features:

- The type t_i : bifurcation or ridge-ending (1bit)
- The coordinates in the image (x_i, y_i) (4bytes)
- The local direction of the associated ridge given by the directional map: θ_i (4bytes)

At the end we have a signature file

$$S_N = \{M_i | i \in \llbracket 1..N \rrbracket \text{ and } M_i = (t_i, x_i, y_i, \theta_i)\}$$

which characterizes the user's fingerprint and whose size is less than 1kB. Compared with the fingerprint image whose size 64kB, we have a high gain in memory requirement. The different steps of the signature extraction from the thinned image are illustrated on the figure below (Fig.17).

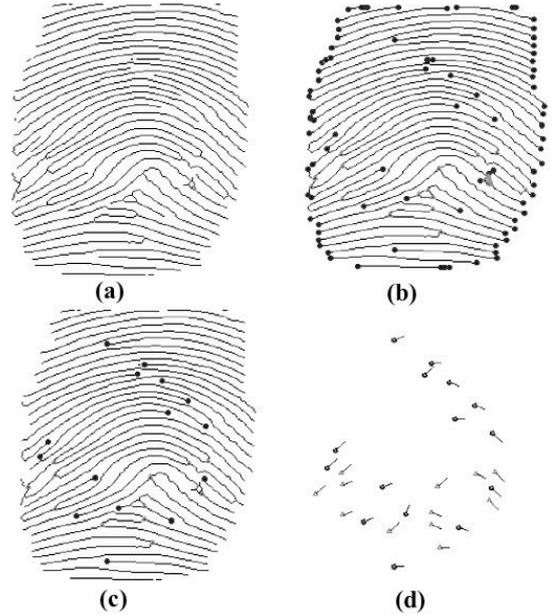


Fig. 18. Illustration of signature extraction from a thinned image (a) : detected minutiae (b), validated minutiae (c) and signature (d).

V. VERIFICATION

Our biometric system is based on verification, i.e. we are seeking to confirm or deny a person's identity compared with a reference record ("Am I who I claim to be?"). We can distinguish two stages: the enrolment and the matching. In course of the enrolment the user's signature S_p is extracted

and stored in memory. Then, at each use, the user's extracted signature S_Q is compared with S_P during the matching step. Naturally these two signatures will always be different, even if they stem from the same user, due to the changes during the acquisition (speed, pressure, dust, skin elasticity...). To overcome this problem sensor distortion is first removed and then a matching score between S_P and S_Q is computed.

Algorithms usually try to find an affine transformation to align S_P on S_Q [28]:

$$\begin{pmatrix} x' \\ y' \\ \theta' \end{pmatrix} = k \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & k^{-1} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ \theta \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \\ \alpha \end{pmatrix} \quad (10)$$

where k , α and $(\Delta x, \Delta y)$ represent the scaling factor, the rotation parameter and the translation between the two fingerprints. In our case the finger moves always along the same direction, so we have no rotation parameter: $\alpha=0$. This model performs well for matrix sensors but is utterly unsuitable for our sweeping mode sensor. Indeed we have seen that our acquisition method can cause image areas with great speed variations, hence a nonlinear factor k . Other mathematical models taking into account nonlinear local distortion created by skin elasticity have been proposed [35]-[38], but they are too long and not adapted for our type of distortion. As $\alpha=0$, we are looking here a transformation like (11) where f and g are nonlinear functions which represent the speed variation in course of a vertical finger moving.

$$\begin{pmatrix} x' \\ y' \\ \theta' \end{pmatrix} = \begin{pmatrix} x \\ f(y) \\ g(\theta) \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \\ 0 \end{pmatrix} \quad (11)$$

A. Distortion modelling

Let us first consider a square block where ridges have roughly the same direction. We are seeking to estimate the local scaling factor k , which enables to get the corresponding block without distortion. In this case we can model the ridges by parallel lines as shown on Fig. 19.

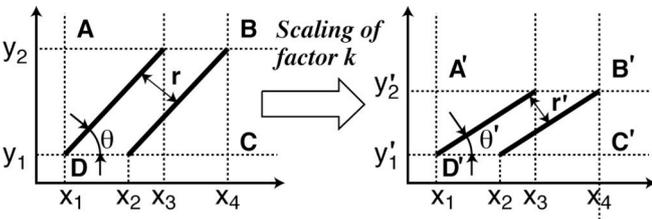


Fig. 19. Local vertical distortion modelling of a block.

By considering the area $ABCD$ and its corresponding scaled area $A'B'C'D'$, we get the two following equations:

$$k \cdot \tan\theta' = \tan\theta \quad (12)$$

$$r' \cdot \sin\theta = r \cdot \sin\theta' \quad (13)$$

Then the scaling factor k can be expressed according to the parameters r , r' and θ :

$$k = \frac{r}{r'} \times \frac{1}{|\cos\theta|} \times \sqrt{1 - \frac{r'^2}{r^2} \sin^2\theta} \quad (14)$$

In the real case the distortion factor $k(x,y)$ is computed for each block (x,y) and has the following form:

$$k(x,y) = \frac{r(x,y)}{r_{global}} \cdot \frac{1}{|\cos\theta(x,y)|} \sqrt{1 - \frac{r_{global}^2}{r(x,y)^2} \sin^2\theta(x,y)} \quad (15)$$

where $r(x,y)$ is the local inter-ridge distance, $\theta(x,y)$ is the local ridge direction, and r_{global} is the average inter-ridge distance in the non-distorted fingerprint image. $r(x,y)$ and $\theta(x,y)$ are given by the estimate of directional and frequential fields. To estimate r_{global} we consider the set V of blocks whose direction is practically vertical:

$$V = \left\{ (x,y) \mid |\sin\theta(x,y)| \geq \cos\theta_{max} \right\} \quad (16)$$

As the finger is moved vertically the inter-ridge distance remains virtually unchanged in these areas. If V has a sufficient number of blocks, then a good estimate of r_{global} can be obtained by an average of ridge separation on V , else r_{global} is replaced by a constant value $R0$:

$$r_{global} = \begin{cases} \frac{1}{\|V\|} \cdot \sum_{(x,y) \in V} r(x,y) & \text{if } \|V\| \geq N_{B_{MIN}} \\ R0 & \text{if } \|V\| < N_{B_{MIN}} \end{cases} \quad (17)$$

We have specified $\theta_{max} = \pi/8$, $N_{B_{MIN}} = 10$ and $R0 = 9 \text{ pixels}$.

Before computing $k(x,y)$ some precautions have to be taken:

If ridges are locally vertical, then the estimate of k is impossible because $r=r'$ on Fig. 19. We have $\theta(x,y)=\pi/2$ and the result of (15) is undefined (division by zero).

$k(x,y)$ is a real number, thus the condition $r(x,y) \geq r_{global} \cdot |\sin\theta(x,y)|$ must be checked. This condition may be false due to errors in estimates of $r(x,y)$ and $\theta(x,y)$, the estimate of k is impossible in this case.

The skin elasticity is insignificant compared with the distortion from the sweeping mode and the finger is moved vertically, we can so consider that $k(x,y)$ is virtually constant for a given line y . For each line we define the average scaling factor k_y (19) by the mean of $k(x,y)$ where they are defined (18).

$$S(y) = \left\{ x \mid \begin{array}{l} r(x,y) \geq r_{global} \times |\sin\theta(x,y)| \\ \text{and } \theta(x,y) \neq \frac{\pi}{2} \end{array} \right\} \quad (18)$$

$$k_y = \begin{cases} \frac{1}{|S(y)|} \sum_{x \in S(y)} k(x,y) & \text{if } S(y) \neq \emptyset \\ 1 & \text{if } S(y) = \emptyset \end{cases} \quad (19)$$

B. Distortion correction

In the previous section we have generated a vertical distortion map where a scaling factor k_y is credited to each image segment of size $L \times H$ (H is the block size and L corresponds to the image width). This enables to reconstruct the non-distorted image by interpolation where each segment has a new height H/k_y , as illustrated on Fig. 20.

Nonetheless this reconstruction is useless at this stage because we now work on the signature file. The latter contains a set of minutiae M_i defined by $(t_i, x_i, y_i, \theta_i)$. By applying the inverse distortion to the minutiae we can obtain the new features $(t_i, x_i, y_i', \theta_i')$. The new vertical coordinate results from (19) such as:

$$\begin{aligned} \exists(p, \Delta y) \in \mathbb{N} \times \llbracket 0, H-1 \rrbracket \mid y = p \times H + \Delta y \\ (x, y) \mapsto (x, f(y)) = (X, Y) \end{aligned} \quad (20)$$

$$f(y) = \int_0^y \frac{1}{k_y} dy = \sum_{i=0}^{p-1} \frac{H}{k_i} + \frac{\Delta y}{k_p}$$

and the new local orientation value can be obtained from (12) and (15) as follows:

$$\begin{aligned} \theta(x, y) \mapsto \Theta(x, y) = g(\theta(x, y)) \\ g(\theta(x, y)) = \tan^{-1} \left(\frac{\tan \theta(x, y)}{k(x, y)} \right) \end{aligned} \quad (21)$$

This model is not perfect because it is not continuous; nonetheless it enables to limit significantly the inter-ridge distance variations for a trained user.

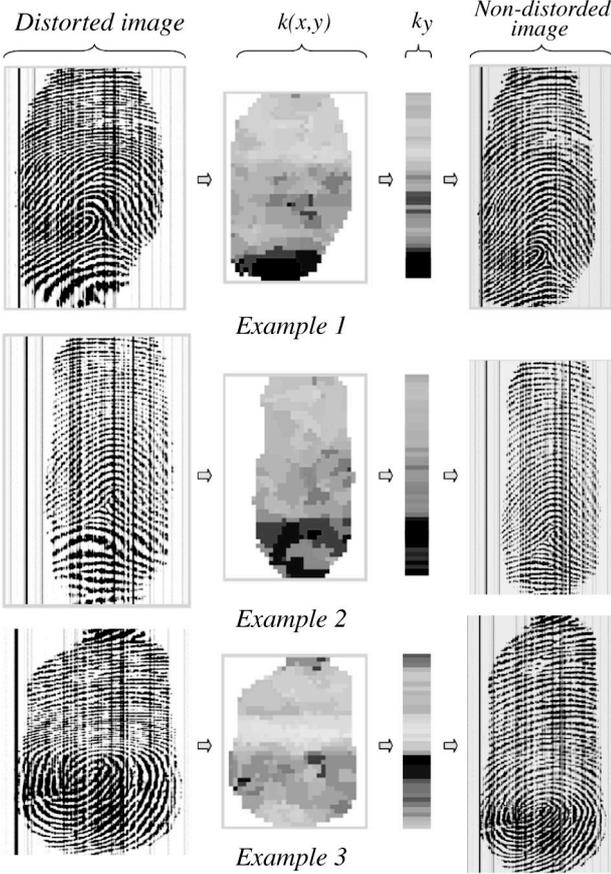


Fig. 20. Examples of reconstruction of undistorted fingerprints from the distortion map (use of bicubic interpolation with Matlab).

C. Enrolment

We have a fingerprint verification system for a single user. This consists in confirming or denying a person's identity compared with a reference record. To initialize the system the rightful user has first to record his signature S_p in memory: this is the enrolment step. The distorted signature S_p is first transformed into its corresponding non-distorted file E_p by means of (20) and (21), and then E_p is stored in memory. We also store the value r_{global}^p (17) that will be used in course of the matching step.

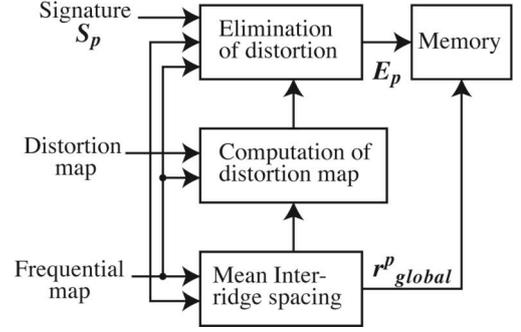


Fig. 21. Enrolment procedure.

To ensure good performance of the verification system, the enrolled image has to satisfy three requirements:

The image height H. Too small or too tall images are difficult to exploit, so we require H to be in the range [200..512].

The number of minutiae. Numerous false minutiae may remain in the case of too noisy images in spite of the pre-processing. According to the histogram of validated minutiae we decided to fix a maximum threshold of 100 minutiae.

The fingerprint area. After the segmentation the remaining surface may be too small to collect enough useful information for verification. We specified a foreground percentage of 60% for enrolment.

Other conditions may be applied by defining a quality factor [39]-[40], but they generate an additional computation time.

D. Matching

Once the enrolment has been performed the system is fully operational. At each use the user's signature S_Q is extracted to be compared to S_p . Two fingerprint images from the same person will of course be always different because they will be never acquired in strict similar conditions (noise, distortion...). Thus a matching score (MS) defining the similarity degree between S_p and S_Q is first computed, and then it is compared to a specified threshold in order to decide if the two signatures come from the same person. Before computing MS , the distortion from S_Q is removed. Due to noise two signatures from the same person may have different ridge spacing, this is why the value r_{global}^p is used to remove the distortion from S_Q .

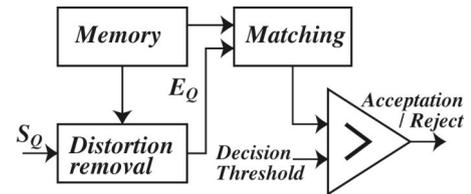


Fig. 22. Matching procedure.

To match two signatures we look to find the best alignment of E_Q on E_p . As the distortion from sweeping mode has been removed, the matching consists in finding the translation $(\Delta x, \Delta y)$ between the two sets:

$$\begin{pmatrix} x^p \\ y^p \\ \theta^p \end{pmatrix} = \begin{pmatrix} x^Q \\ y^Q \\ \theta^Q \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \\ 0 \end{pmatrix} \quad (\text{Eq.22})$$

The matching algorithm follows the 5 following steps:

We are looking for a minutiae reference pair $(M_{i_r}^P, M_{j_r}^Q) \in E_P \times E_Q$. To be a reference these two minutiae must have the same type ($t_{i_r}^P = t_{j_r}^Q$) and a roughly similar direction defined by $|\sin(\theta_{i_r}^P - \theta_{j_r}^Q)| < \sin(\theta_{MAX}^R)$ and $\theta_{MAX}^R = 10^\circ$. We have used a rigorous condition in order to limit calculations and potential candidates.

The translation vector $T[\Delta x, \Delta y]$ between $M_{j_r}^Q$ and $M_{i_r}^P$ is computed: $\Delta x = x_{j_r}^Q - x_{i_r}^P$ and $\Delta y = y_{j_r}^Q - y_{i_r}^P$.

E_Q is then aligned on E_P with respect to the reference pair by the transformation $T[\Delta x, \Delta y]$ and we are looking for the matched minutiae. Two minutiae will unlikely overlap, thus we associate a bounding box of rectangular size $L \times H$ at each M_i^P . M_j^Q matches to M_i^P if it falls into the box associated to M_i^P , i.e. if it checks (23). We have empirically determined $[L, H] = [10, 16]$ where H is larger than L to face with possible errors in distortion map.

$$[M_i^P \equiv M_j^Q] \Leftrightarrow \begin{cases} |x_i^P + \Delta x - x_j^Q| \leq L/2 \\ |y_i^P + \Delta y - y_j^Q| \leq H/2 \end{cases} \quad (23)$$

For each matched pair we associate the quality factor $q_k = (1 - |\sin \Delta \theta_{ij}|)^2$ with $\Delta \theta_{ij} = \theta_i^P - \theta_j^Q$

Once we have found all matched pairs, we compute the corresponding quality value $q_{i_r, j_r} = \sum_{k=1}^m q_k$ which is the sum of quality factors.

The four previous steps are executed for each reference pair and finally we compute $Q = \max_R(q_{i_r, j_r})$ which corresponds to the best alignment between the two signatures.

Q represents the similarity degree between E_P and E_Q . A matching score is then computed according to $|E_P|$, $|E_Q|$ and Q (24), and it is compared to a fixed threshold λ to decide if the user is authorized or not (the choice of threshold depends on the security settings of the intended application).

$$MS = Q / \max(|E_P|, |E_Q|) \quad (24)$$

The choice of formula to compute MS may affect the performance of the system [41]. Different usual formulae were tested, but (24) gave the best results.

VI. PERFORMANCE

Due to the part of uncertainty in course of the matching, the decision to accept or reject a user may be erroneous. The performance evaluation consists in studying statistically the frequency of these incorrect decisions on a given fingerprint database [42]. Here the database (TDB) has been obtained by means of our sweep sensor and the acquisition driver described in section II, and it contains a set of 200 fingerprint images which have been collected from 20 different fingers with 10 samples per finger [20]. Three artificial databases have also been synthesized for tests by means of a fingerprint generator and a sensor modelling:

- SDB1 represents the ideal case for a sweep sensor by both cooperative and trained users. Images are featured by a good placement of the finger and slight speed variations.

- SDB2 contains extreme cases with a bad placement of

the finger (laterally or longitudinally).

- SDB3 simulates sudden and great speed variations in course of the acquisition.

The use of artificial data is interesting as it enables a gain of time, an easy use and the simulation of extreme cases [43]-[44].

By computing the matching scores between the different pairs of fingerprint images from database, two kinds of error can be highlighted [45] according to the threshold decision t :

- The *False Matching Rate* ($FMR(t)$): this corresponds to the percentage of unauthorized users who are accepted by the system.

- The *False Non-Matching Rate* ($FNMR(t)$): this corresponds to the percentage of authorized users who are rejected by the system.

- The *Receiving Operating Characteristics curve* (ROC), expressing $FNMR(t)$ according to $FMR(t)$ on a logarithmic scale, is then plotted to summarize the system performance and to compare results from different databases or algorithms. The results from our four databases are illustrated on Fig. 23.

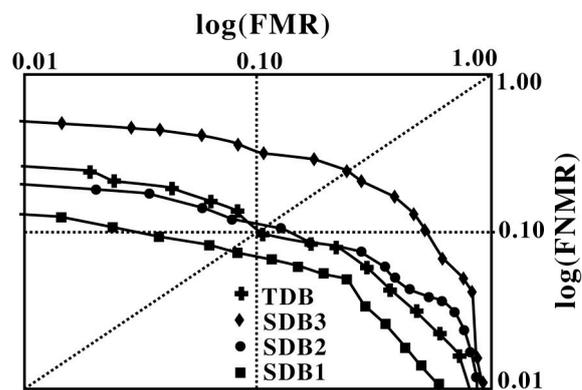


Fig. 23. Roc curves obtained from the four databases.

As SDB1 represents the ideal case, it gives the best results. SDB2 gives lower performance; a bad placement of the finger may reduce the number of detected minutiae but also the lower fingerprint area makes more difficult the matching stage. SDB3 shows the limits of the distortion model applied to blocks and which is not continuous. If the speed changes are sharp or happens frequently during an acquisition, then the model is unable to handle efficiently the distortion. The resulting inter-ridge spacing and performance are altered. We see that TDB gives results roughly similar to SDB2. Users had first undergone a training stage before collecting their fingerprints for database creation. This short training stage allows capturing fingerprints with less irregular movements like the ones contained in SDB3. Nonetheless bad placements of the finger, particularly the lateral ones, are made unavoidable in the current conditions. This may be avoided by using a guiding system that would prevent the finger from going beyond sides of sensor.

Finally there is a noteworthy point on the ROC curve where FMR is equal to $FNMR$: the *Equal Error Rate* (EER). EER represents the best trade-off between FMR and $FNMR$, and so it is sometimes used to give an idea about overall performance. However it has to be pointed out that in practice the efficiency of the system is narrowly linked to the intended application. Indeed high security settings

require low FMR to limit the acceptance of unauthorized users, whereas user convenience requires low $FNMR$ to limit the rejection of authorized users. Consequently EER is not representative of performance from a particular application and is not a good choice to tune a system. Here we have $EER=10.1\%$ for TDB, this result is still far from those of state of the art algorithm but it is encouraging as the sensor is currently still at the experimental state.

VII. CONCLUSIONS

In this work we have developed a full fingerprint verification system based on minutiae features. This system employs a new kind of sweep sensor that uses a tactile measure of the fingerprint and has only a one-pixel row to acquire the image. These two particularities may cause a great image distortion according to the user's behavior and require a specific treatment to process images. To get rid of this distortion a bank of directional Log-Gabor masks have been used and a new distortion model has been implemented. Performance evaluation has given encouraging results and has shown that some improvements have to be made regarding the quality of images produced by the sensor.

We are still coping with weakness of cantilevers and break of the later caused by high finger pressure (vertical line effect) or during fabrication. We are now focusing on new solutions to package efficiently the sensor. This will enable to improve image quality and to get better performance. Another encountered difficulty is the great distortion caused by the sweeping mode. Although the implemented distortion modeling performs well, this is not perfect especially in extreme cases. Minutiae features used by our system (i.e. position and direction) are very sensitive to speed changes, that is the reason why researches will be carried out in a near future to use more robust characteristics (e.g. the number of ridges between two minutiae). A specialized hardware device, which would measure the finger speed, is also under consideration in order to reconstruct directly the image with limited distortion at the expense of the price of the sensor chip.

REFERENCES

- [1] A.K. Jain, L. Hong and S. Pankanti, "Biometrics: Promising Frontiers for Emerging Identification Market", *Comm. ACM*, pp. 91-98, February 2000.
- [2] International Biometric Group, homepage: www.biometricgroup.com
- [3] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", *IEEE Transactions on PAMI*, Vol. 24, No. 8, pp. 1010-1025, 2002.
- [4] A. Ross and A. Jain, "Biometric Sensor Interoperability: A Case Study In Fingerprints", *Proc. of International ECCV Workshop on Biometric Authentication (BioAW)*, (Prague), LNCS vol. 3087, pp. 134-145, Springer Publishers, May 2004.
- [5] H. Morimura, S. Shigematsu, and K. Machida, "A Novel Sensor Cell Architecture and Sensing Circuit Scheme for Capacitive Fingerprint Sensors", *IEEE Journal Of Solid-State Circuits*, Vol. 35, No. 5, May 2000.
- [6] S. Jung, R.Thewes, T. Scheiter, K.F. Goser and W. Weber, "A Low-Power and High-Performance CMOS Fingerprint Sensing and Encoding Architecture", *IEEE Journal of Solid-State Circuits*, Vol. 34, No. 7, pp. 978-984, July 1999.
- [7] J.W. Lee, D.JMin, J.Kim, and W. Kim, "A 600-dpi Capacitive Fingerprint Sensor Chip and Image-Synthesis Technique", *IEEE Journal of Solid-State Circuits*, Vol. 34, No. 4, pp. 469-475, April 1999.
- [8] M. Tartagni and R. Guerrieri, "A Fingerprint Sensor Based on the Feedback Capacitive Sensing Scheme", *IEEE Journal Of Solid-State Circuits*, Vol. 33, No. 1, January 1998.
- [9] O. Vermesan et al., "A 500-dpi AC capacitive hybrid flip-chip CMOS ASIC/sensor module for fingerprint, navigation, and pointer detection with on-chip data processing", *IEEE Journal of Solid-State Circuits*, Vol.38, Issue 12, pp.:2288-2296, December 2003.
- [10] J.F. Mainguet, M. Pégulu and J.B. Harris, "Fingerprint recognition based on silicon chips", *Future Generation Computer Systems*, pp. 403-415, December 2000.
- [11] J.S. Han, T. Kadowaki, K. Sato and M. Shikida, "Thermal analysis of fingerprint sensor having a microheater array", *Proceedings of International Symposium on Micromechatronics and Human Science*, 1999.
- [12] R.W. Sandage and J.A. Connely, "A Fingerprint Opto-Detector Using Lateral Bipolar Phototransistors in a Standard CMOS Process", *IEDM'95*, pp. 171-174, 1995.
- [13] N.D. Young, G. Harkin, R.M. Bunn, D.J. McCulloch, R.W. Wilks and A.G. Knapp, "Novel Fingerprint Scanning Arrays Using Polysilicon TFT's on Glass and Polymer Substrates", *IEEE Electron Device Letters*, Vol. 18, No. 1, January 1997.
- [14] R.J. De Souza and K.D. Wise, "A Very High Density Bulk Micromachined Capacitive Tactile Imager", *International Conference on Solid-State Sensors and Actuators, Transducers '97*, Chicago, June 16-19, 1997.
- [15] P. Rey, P. Charvet, M.T. Delaye and S. Abou Hassan, "A High Density Capacitive Pressure Sensor Array For Fingerprint Sensor Application", *International Conference on Solid-State Sensors and Actuators, Transducers '97*, Chicago, June 16-19, 1997.
- [16] <http://cmp.imag.fr/>
- [17] J.F. Mainguet. "Fingerprint-Reading System", United States Patent No. US 6,289,114 B1, September 2001.
- [18] B. Charlot, F. Parrain, N. Galy, S. Basrouir and B. Courtois, "A Sweeping Mode Integrated Fingerprint Sensor With 256 Tactile Microbeams", *IEEE Journal of Microelectromechanical Systems*, Vol 13, Issue 4, pp. 636-644, 2004.
- [19] APEX 20k200E development board from Altera company, website: www.altera.com
- [20] Micro and Nano System Group from TIMA laboratory, homepage: <http://tima.imag.fr/mns>
- [21] A.M. Bazen and S.H. Gerez, "Segmentation of Fingerprint Images", in *12th Annual Workshop on Circuits, Systems and Signal Processing*, pp. 276-280, Veldhoven, The Netherlands, November 2001.
- [22] H. Ailisto, M. Lindholm and P. Tikkanen, "A review of fingerprint image enhancement methods", *International Journal of Image and Graphics*, Vol. 3, No. 3, pp. 401-424, 2004.
- [23] A.K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "FingerCode: A Filterbank for Fingerprint Representation and Matching", *Proc. IEEE Conference on CVPR*, Vol. 2, pp. 187-193, Colorado, June 23-25, 1999.
- [24] H. Hong, Z. Hong and W. Le-yu, "Optimal design of Gabor filters for fingerprint recognition", *Proceedings of the SPIE*, Vol. 4790-85, pp. 351-356, Seattle, Washington, USA, Annual Meeting 2002.
- [25] J. Yang, L. Liu, T. Jiang and Y. Fan, "A modified Gabor filter design method for fingerprint image enhancement", *Pattern Recognition Letters*, Vol. 24, No 12, pp. 1805-1817, 2003.
- [26] L. Hong, Y. Wan and A.K. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", *IEEE Trans. On Pattern Analysis and Machine Intelligence*, Vol. 20, No. 8, pp. 777-789, August 1998.
- [27] D.J. Field, "Relations between the statistics of natural images and the response properties of cortical cells", *Journal of the Optical Society of America*, Vol. 4, No. 12, pp. 2379-2394, December 1987.
- [28] N. Yager and A. Amin, "Fingerprint verification based on minutiae features: a review", *Pattern Analysis and Applications*, Vol. 7, Issue 1, pp. 94-113, 2004.
- [29] R. Stefanelli and A. Rosenfeld, "Some parallel thinning algorithms for digital pictures", *Journal of the ACM*, Vol.18, No2, pp.255-264, April 1971.
- [30] L.Lam, S.W. Lee and C.Y. Suen, "Thinning Methodologies-A Comprehensive Survey", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 14, Issue 9, pp. 869-885, September 1992.
- [31] Y.Y. Zhang and P.S.P. Wang, "Design of Parallel Thinning Algorithms", *Proceedings of the 3rd International Workshop on Parallel Image Analysis*, pp. 183-194, College Park, 1994.
- [32] Z. Bian, D. Zhang and W. Shu, "Knowledge-Based Fingerprint Post-Processing", *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 16, No.1, pp. 53-67, 2002.

- [33] S. Kim, D. Lee and J. Kim, "Algorithm for Detection and Elimination of False Minutiae in Fingerprint Images", *Lecture Notes in Computer Science*, Springer Verlag, Vol. 2091, pp. 235-240, 2001.
- [34] A. Farina, Z.M. Kovács-Vajna and A. Leone, "Fingerprint minutiae extraction from skeletonized binary images", *Pattern Recognition*, Vol. 32, pp. 877-889, 1999.
- [35] R.Cappelli, D.Maio and D.Maltoni, "Modelling Plastic Distortion in Fingerprint Images", Proceedings of the 2nd International Conference on Advances in Pattern Recognition, Rio de Janeiro, pp.369-376, 2001.
- [36] A. Ross, S. Dass and A. Jain, "A deformable model for fingerprint matching", *Pattern Recognition*, Vol. 38, pp. 95-103, 2005.
- [37] A.M. Bazen and S.H. Gerez, "Fingerprint matching by thin-plate spline modelling of elastic deformations", *Pattern Recognition*, Vol. 36, pp. 1859-1867, 2003.
- [38] A.Senior, R.Bolle, "Improved Fingerprint Matching by Distortion Removal", *IEICE Transactions on Information and Systems*, pp. 825-831, 2001.
- [39] E. Lim, X. Jiang and W. Yau, "Fingerprint Quality And Validity Analysis", *IEEE Proceedings of International Conference on Image Processing*, Vol. 1, pp. 469-472, 2002.
- [40] M.Y. Yao, S. Pankanti, N. Haas, N.K. Ratha and R.M. Bolle., "Quantifying Quality: A Case Study in Fingerprints", *Proceedings of IEEE Conference on AutoID*, pp.126-131, March 2002.
- [41] R.M. Bolle, J.H. Connell, N.K. Ratha, "Biometrics perils and patches", *Pattern Recognition*, Vol. 35, pp. 2727-2738, 2002.
- [42] D.Maio, D. Maltoni, R. Cappelli, J.L. Wayman and A.K. Jain, "FVC2000: Fingerprint Verification Competition", *IEEE PAMI*, vol. 24, No. 3, pp. 402-412, March 2002.
- [43] S. Yanushkevich, A. Stoica, S. Srihari, V. Shmerko and M. Gavrilova, "Simulation of Biometric Information: The New Generation of Biometric Systems", *Proceedings of the International Workshop on Modeling and Simulation on Biometric Technologies*, Calgary, Canada, pp. 87-98, 22-23 June 2004.
- [44] T. Ayers, R. Federkeil, T. Nichols and R. Parmar, "Modeling Fingerprints: Components for the Task of Synthesis", *Proceedings of the International Workshop on Modeling and Simulation on Biometric Technologies*, Calgary, Canada, pp. 155-162, 22-23 June 2004.
- [45] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy Magazine*, Vol. 1, No. 2, pp. 33-42, March-April 2003.



Nicolas Galy was born in Colmar, France in 1977. He received M.S from the Ecole National Supérieur d'Electricité et de Radioelectricité de Grenoble, France in 2001 and Ph.D from The Institut National Polytechnique de Grenoble, France in 2005. His research interest concerns image processing for fingerprint recognition. He is currently works in a consulting company in image processing



Benoît Charlot was born in Vichy, France, in 1972. He received M.S and Ph.D degrees in microelectronics from the Institut National Polytechnique de Grenoble, France in 1996 and 2001, respectively. He is currently a researcher of the CNRS (the French National Centre of the Scientific Research) at LIMMS laboratory in Tokyo, Japan. Until mid 2005 he was researcher in TIMA laboratory, Grenoble, France. His research areas concerns fingerprint sensors, micro power generators, nanomechanical memories and field emission for RF MEMS. He is reviewer for IEEE journal of Micromechanical sensors.



Bernard Courtois (M'00) was born in Paris, France, in 1948. He received the M.S. degree in engineering from the Ecole Nationale Supérieure d'Informatique et Mathématiques Appliquées de Grenoble, Grenoble, France, in 1973 and the Dr.Ing. and Dr.Sci. degrees from the Institut National Polytechnique de Grenoble, Grenoble, France. He is currently Director of the Laboratory of Techniques of Informatics and Microelectronics, Computer Architecture (TIMA), where researches include CAD, architecture and testing of integrated circuits and systems. He is also the Director of CMP Service that is servicing Universities and Companies from about 40 countries for ICs, MCMs, and MEMS prototyping and small volume production. He has been General Chair or Program Chair of various international conferences and workshops, including EDAC-ETC-EUROASIC, Electron and Optical Beam Testing, EUROCHIP, Mixed-Signal Testing, Rapid System Prototyping, THERMINIC and Design, and Test and Microfabrication of MEMS/MOEMS. Dr. Courtois is a member of ACM, ASME, and IMAPS. He is a IEEE Computer Society's Golden Core member and is Doctor Honoris Causa of the Technical University of Budapest.