

# Fake Fingerprint Detection by Odor Analysis\*,\*\*

Denis Baldisserra, Annalisa Franco, Dario Maio, and Davide Maltoni

DEIS, Università di Bologna,  
Viale Risorgimento 2, 40136 Bologna, Italy  
{baldisse, franco, maio, maltoni}@csr.unibo.it

**Abstract.** This work proposes a novel approach to secure fingerprint scanners against the presentation of fake fingerprints. An odor sensor (electronic nose) is used to sample the odor signal and an ad-hoc algorithm allows to discriminate the finger skin odor from that of other materials such as latex, silicone or gelatin, usually employed to forge fake fingerprints. The experimental results confirm the effectiveness of the proposed approach.

## 1 Introduction

Although the recognition performance of state-of-the-art biometric systems is nowadays quite satisfactory for most applications, much work is still necessary to allow convenient, secure and privacy-friendly systems to be designed. Fingerprints represent today one of the most used biometric characteristics in human recognition systems, due to its uniqueness and reliability. Some recent studies [6] [5] have shown that most of the fingerprint-based recognition systems available on the market can be fooled by presenting to the sensing device a three-dimensional mold (such as a rubber membrane, glue impression, or gelatin finger) that reproduces the ridge characteristics of the fingerprint. While manufacturing a fake finger with the cooperation of the finger owner is definitely quite easy, producing a sufficient quality clone from a latent fingerprint is significantly more difficult; in any case adequate protections have to be studied and implemented to secure the new generation of fingerprint sensing devices.

In the literature, some approaches have been recently presented to deal with the above problem which is often referred to as “fingerprint aliveness detection”, i.e. the discrimination of a real and live fingerprint from a fake or deceased one. Some approaches use ad-hoc extra-hardware to acquire life signs such as the epidermis temperature [6], the pulse oximetry and the blood pressure [7], or other properties such as the electric resistance [6], optical characteristics (absorption, reflection, scattering and refraction) or dielectric permittivity [5]. Unfortunately, the performance achieved by most of these methods is not satisfactory, due to the inherent variability of such characteristics. Another aliveness detection method has been recently proposed in [1] where a sequence of fingerprint images is analyzed to detect the perspiration process that typically does not occur in cadaver or artificial

---

\* This work was partially supported by European Commission (BioSec - FP6 IST-2002-001766).

\*\* Patent Pending (IT #BO2005A000398).

fingerprints. It is worth noting that, since the only aim of the aliveness detection module is to verify if the fingerprint is real, and not to verify/identify the user, the module is usually integrated into a more complete verification/identification system where aliveness detection is often executed before user recognition.

In this work a new aliveness detection approach based on the odor analysis is presented. The paper is organized as follows: in section 2 a brief introduction to electronic odor analysis is given, in section 3 the hardware system designed for odor acquisition is presented; section 4 describes the odor recognition approach while section 5 reports the experimental results; finally, in section 6, some concluding remarks are given.

## 2 Electronic Odor Analysis

Everything that has an odor constantly evaporates tiny quantities of molecules, the so called odorants; a sensor able to detect these molecules is called *chemical sensor*. An *electronic nose* is an array of chemical sensors designed to detect and discriminate several complex odors. Odor stimulation to the sensing system produces the characteristic pattern of an odor. Since the strength of the signal in most sensors is proportional to the concentration of a compound, quantitative data can be produced for further processing. Electronic noses are equipped with hardware components to collect and transport the different odors to the sensor array, as well as electronic circuits to digitize and store the sensor response for subsequent signal processing.

Several *electronic noses* are nowadays available on the market [2]. The main applications where electronic noses are employed are [3]: medical diagnosis, environmental applications to identify toxic and dangerous escapes, systems aimed to assess quality in food production and pharmaceutical applications.

Although “odor recognition” is not a novel modality in the biometric system arena (see for example [4]), to the best of our knowledge this is the first approach where the finger odor is used to detect fake fingerprints.

## 3 The Odor Acquisition System

### 3.1 The Odor Sensors and the Acquisition Board

Different odor sensors, based on metal-oxide technology (MOS), have been tested in our experiments. Some of these sensors are available in the market (Figaro TGS 2600, Figaro TGS 822, FIS SB-31, FIS SB-AQ1A), other sensors are prototypes produced by an Italian company (SACMI) which is currently developing electronic noses for the food industry. Each of these sensors reacts to some odors while ignoring others: some of them are designed to detect gaseous air contaminants, other are designed to detect organic compounds, etc. All the sensors can be miniaturized enough (few mm<sup>2</sup>) to be embedded into very small devices, and the sensor cost is quite small for volume productions (few €).

An electronic board has been developed<sup>1</sup> to drive the different odor sensors and to acquire the odor signals through a PC; the board allows to: 1) heat the sensors to make them working at the proper temperature (200 – 400 °C); 2) tune and modify the sensors operating point, the offset and to compensate for thermal deviation; 3) pre-amplify and pre-elaborate the signals provided by the MOS sensors; 4) convert (A/D) the pre-amplified analog signals into (10-bit resolution) digital signals; 5) sample the odor signal (of the pre-selected sensor) every few ms and send it to a PC via RS-232 interface. It is worth noting that embedding MOS odor sensors into a fingerprint scanner is not straightforward and special care must be taken to guarantee that the same part of skin which is sensed for identity verification is also sensed for odor analysis.

### 3.2 The Acquisition Process

The acquisition of an odor pattern consists of sampling the data coming from an odor sensor during a given time interval, usually few seconds. A typical acquisition session is composed of three different stages: calibration, recording and restoration.

When the system is idle (i.e., there are no fingers placed on the sensor surface), it periodically read data from the electronic board to establish (and update) a baseline response, denoted as “response in fresh air”. This operation, called *calibration*, is continuously performed in background since the prototype version of the system works in an open environment and the sensors are thus exposed to environmental changes (e.g. breathing close to the odor sensors or accidental sprinkling of particular substances). The *recording* stage measures the sensor response when a finger is placed on the sensor surface. The user’s finger has to be placed on the odor sensor surface for a few seconds and then lifted. Finally, the *restoration* stage starts when the finger is lifted from the sensor surface and is aimed at restoring the sensor to its initial conditions. The time necessary to restore the sensor response may vary depending on the sensor characteristic and environmental condition (a typical time interval for the sensors used is 10-15 seconds).

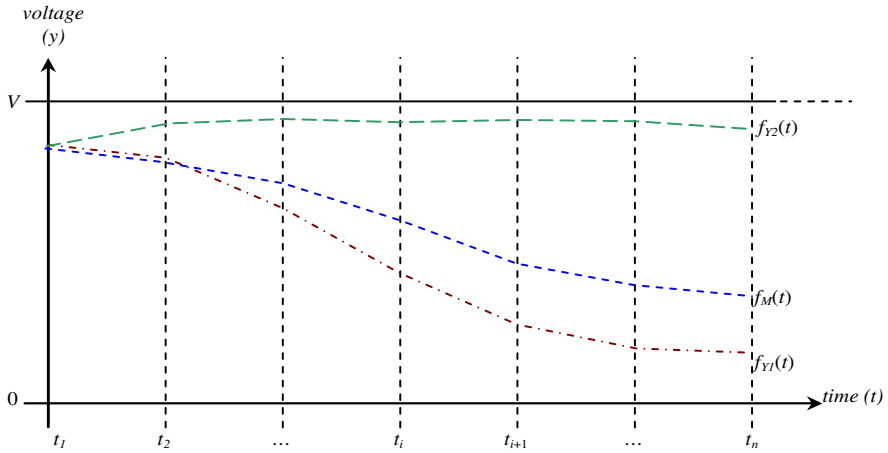
## 4 Odor Recognition

### 4.1 Data Processing

Let  $X$  be an acquisition sequence consisting of  $n$  sensor readings  $X = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n\}$ ; each reading is represented by a two dimensional vector  $\mathbf{x}_i = [x_i^t, x_i^v]^T$  where  $x_i^t$  denotes the elapsed time since the beginning of the acquisition and  $x_i^v$  the recorded voltage ( $x_i^v \in [0, V]$ , where  $V=5$  in our acquisition system). The first sample is acquired at the beginning of the acquisition stage; the acquisition covers all the recording stage (5 seconds) and the first 8 seconds of the restoration stage. The

---

<sup>1</sup> The electronic board has been developed by the Italian company Biometrika, which is one of the DEIS (University of Bologna) partners in the BioSec project (IST-2002-001766).



**Fig. 1.** Three piecewise linear functions  $f_M(t)$ ,  $f_{Y1}(t)$  and  $f_{Y2}(t)$  representing the stored user's template  $M$  and the acquisition sequences of two artificial fingerprints ( $Y_1$  and  $Y_2$ ) forged using gelatine and silicone respectively

sampling frequency is about 100 Hz. The acquired sequence is then interpolated and downsampled in order to: 1) obtain the voltage values at predefined and regular intervals of width  $\Delta t$  (200 ms in our experiment); 2) partially smooth the data and reduce noise. The processed sequence  $Y = \{y_1, y_2, \dots, y_n\}$  has length  $n$  and each element  $y_i$  represents the voltage value at time  $t_i = t_1 + i \cdot \Delta t$ . We indicate with  $f_Y(t)$  the piecewise linear function interpolating the sequence  $Y$ , obtained by connecting each couple of consecutive points  $(y_i, y_{i+1})$  by a straight line (see Fig. 1).

A template, consisting of an acquisition sequence  $M = \{m_1, m_2, \dots, m_n\}$ , represented by the piecewise linear function  $f_M(t)$ , is created for each new user enrolled into the system. The aliveness verification of a user fingerprint is carried out by comparing the function  $f_Y(t)$  and  $f_M(t)$  representing the newly acquired data  $Y$  and the user's stored template  $M$  respectively. The comparison between the two functions is based on the fusion of three different features extracted from the sequences: the function trend, the area between the two functions and the correlation between the two data sequences. The three similarity values are combined to produce the final decision.

#### 4.1.1 Function Trend

Some preliminary experiments showed that, when the odor sensors are exposed to skin or gelatin, the acquired voltage gradually decreases, while when exposed to other substances such as silicone or latex the voltage increases (see Fig. 1); analyzing the trend of the curve, allows a first distinction between these two groups of compounds to be made. The trend is analyzed on the basis of the angle between the two functions and the horizontal axis. The angle  $\alpha_i$  between  $f_M(t)$  and the horizontal axis, in the

interval  $[t_i, t_{i+1}]$ , is calculated as:  $\alpha_i = \arctan\left(\frac{f_M(t_i) - f_M(t_{i+1})}{\Delta t}\right)$

The angle  $\beta_i$  of  $f_Y(t)$  in the interval  $[t_i, t_{i+1}]$  is computed analogously. Intuitively the similarity value should be higher if the two functions are concordant (both increasing or both decreasing in the considered interval), and lower otherwise. The similarity  $s_i^{trend}$  is thus calculated as follows:

$$s_i^{trend} = \begin{cases} 1 - (|\alpha_i - \beta_i| + \pi) / 2\pi & \text{if } ((\alpha_i > 0) \text{ and } (\beta_i < 0)) \text{ or } ((\alpha_i < 0) \text{ and } (\beta_i > 0)) \\ 1 - (|\alpha_i - \beta_i|) / 2\pi & \text{if } ((\alpha_i > 0) \text{ and } (\beta_i > 0)) \text{ or } ((\alpha_i < 0) \text{ and } (\beta_i < 0)) \end{cases}$$

The overall trend similarity is given by a simple average of the similarity values  $s_i^{trend}$  over all the intervals:  $s^{trend} = \sum_{i=1}^n s_i^{trend} / n$ . Please note that, since  $s_i^{trend} \in [0,1]$ , the overall similarity  $s^{trend}$  is a value in the interval  $[0,1]$  as well.

#### 4.1.2 Area Between the Two Functions

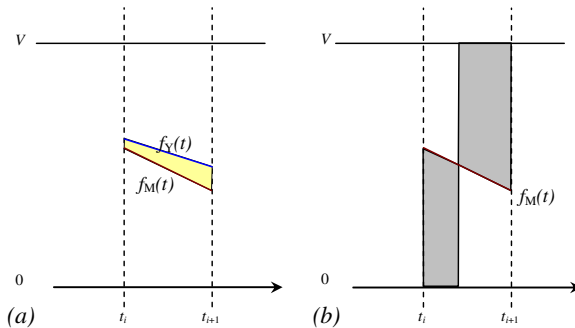
For a single interval  $[t_i, t_{i+1}]$  the area between  $f_Y(t)$  and  $f_M(t)$  is defined as:

$$d_i = \int_{t_i}^{t_{i+1}} |f_Y(t) - f_M(t)| dt$$

The piece-wise form of the two functions (see Fig. 1) allows a simple expression to be derived for  $d_i$ :  $d_i = \left| \frac{\Delta t}{2} \cdot (f_Y(t_i) + f_Y(t_{i+1})) - \frac{\Delta t}{2} \cdot (f_M(t_i) + f_M(t_{i+1})) \right|$

Since the voltage values are constrained to the interval  $[0, V]$ , a local upper bound  $d_i^{UB}$  to the distance from the template function  $f_M(t)$  in the interval  $[t_i, t_{i+1}]$  can be estimated as the maximum area between  $f_M(t)$  and the two horizontal axis of equation  $f(t)=0$  and  $f(t)=V$  (maximum voltage value) respectively:

$$d_i^{UB} = \int_{t_i}^{t_{i+1}} \max(f_M(t), V - f_M(t)) dt$$



**Fig. 2.** (a) Distance in terms of area between the user's template M, approximated by the function  $f_M(t)$ , and the current input Y represented by  $f_Y(t)$ ; (b) local upper bound  $d_i^{UB}$  (grey area) to the distance from the template function  $f_M(t)$  in the interval  $[t_i, t_{i+1}]$

In Fig. 2a an example of the distance between the user's template and the current input is given; in Fig. 2b the area representing the normalization factor is highlighted. The similarity in terms of area between the two functions in a generic interval  $[t_i, t_{i+1}]$  is then simply defined as:  $s_i^{area} = 1 - \frac{d_i}{d_i^{UB}}$ . The overall similarity in the interval  $[t_1, t_n]$

is calculated by averaging the similarity values  $s_i^{area}$  over all the intervals:

$$s^{area} = \sum_{i=1}^n s_i^{area} / n.$$

#### 4.1.3 Correlation

The correlation is a useful statistical indicator that measures the degree of relationship between two statistical variables represented in this case by the two data sequences Y and M. Let  $\bar{y}$  ( $\bar{m}$ ) and  $\sigma_Y$  ( $\sigma_M$ ) be the mean value and the standard deviation of the data sequence Y (M) respectively. The correlation between the two data sequences, considering the whole interval  $[t_1, t_n]$  is simply defined as:

$$\rho_{Y,M} = \frac{\frac{1}{n} \sum_{i=1}^n (y_i - \bar{y})(m_i - \bar{m})}{\sigma_Y \cdot \sigma_M}$$

Since the correlation value  $\rho_{Y,M}$  lies in the interval  $[-1,1]$ , a similarity value in the interval  $[0,1]$  is derived by the simple formula  $s^{corr} = (\rho_{Y,M} + 1)/2$ .

#### 4.1.4 Final decision

Let  $w^{trend}$ ,  $w^{area}$  and  $w^{corr}$  be the weights assigned to the trend, the area and the correlation similarities respectively. The final score is calculated as the weighted average of the three values:  $s = w^{trend} \cdot s^{trend} + w^{area} \cdot s^{area} + w^{corr} \cdot s^{corr}$

The fingerprint is accepted as a real one if the final score  $s$  is higher than a predefined threshold  $thr$ .

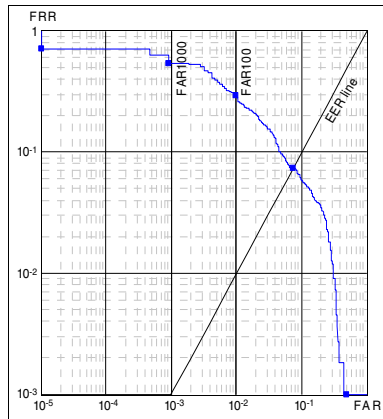
## 5 Experimental Results

In this section the experiments carried out in order to evaluate the fake fingerprint detection approach are presented. Though several odor sensors have been considered in this work, for the sake of brevity only the results obtained by one of the most promising sensors (FIGARO TGS 2600) are here detailed. The database used for testing consists of 300 acquisitions of real fingerprints obtained by capturing 10 odor samples of 2 fingers for each of the 15 volunteers, and 90 acquisitions of artificial fingerprints obtained by capturing 10 odor samples of 12 fingerprints forged using different compounds (3 using the bi-component silicone Prochima RTV 530, 3 using natural latex and 3 using gelatine for alimentary use). An additional validation set, whose acquisitions have not been subsequently used for testing, has been acquired to

tune the parameters of the algorithm. It consists of 50 acquisitions of real fingerprints, obtained by capturing 5 odor samples of 2 fingers for each of the 5 volunteers, and 30 acquisitions of artificial fingerprints obtained by capturing 10 odor samples of 3 artificial fingerprints forged each using one of the materials described above. The system was tested by performing the following comparisons:

- *genuine recognition attempts*: the template of each real fingerprint is compared to the remaining acquisitions of the same finger, but avoiding symmetric matches;
- *impostor recognition attempts*: the template of the first acquisition of each finger is compared to all the artificial fingerprints.

Then the total number of genuine and impostor comparison attempts is 1350 and 2700, respectively. The parameters of the method, tuned on the validation set, have been fixed as follows:  $w^{trend}=0.3$ ,  $w^{area}=0.5$ ,  $w^{corr}=0.2$ . The equal error rate (EER) measured during the experiments is 7.48%, corresponding to a threshold  $thr=0.9518$ . In **Fig. 3** the ROC curve, i.e. false rejection rate (FRR) as a function of false acceptance rate (FAR), is reported. An analysis of the results show that, while it's relatively easy to detect fake fingerprints forged using some materials such as silicone, some problems persist in presence of other compounds (e.g. gelatine) for which the sensor response is similar to that obtained in presence of human skin. Since different sensor present different responses to a particular material, a possible solution to this problem is the combination of data acquired by different odor sensors to obtain a more robust system.



**Fig. 3.** ROC curve of the proposed approach

## 6 Conclusions

In this work a new approach to discriminate between real and fake fingerprints is proposed. The method is based on the acquisition of the odor by means of an electronic nose, whose answer in presence of human skin differs from that obtained in presence of other materials, usually employed to forge artificial fingerprints. The

experimental results confirm that the method is able to effectively discriminate real fingerprints from artificial reproductions forged using a wide range of materials.

As to future research, we intend to investigate other similarity measures to compare the user's template with the current input. Moreover the creation a single model of human skin, instead of a template for each user, will be evaluated.

## References

- [1] Derakhshani R., Scuckers S., Hornak L., O'Gorman L., "Determination of Vitality From A Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners", *Pattern Recognition*, vol. 17, no. 2, pp. 383-396, 2003.
- [2] Harwood D., "Something in the air", *IEE Review*, vol. 47, pp. 10-14, 2001.
- [3] Keller, P. E., "Electronic noses and their applications", *IEEE Technical Applications Conference and Workshops Northcon*, pp. 116- 120, 1995.
- [4] Korotkaya Z., "Biometric Person Authentication: Odor", available at <http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf>
- [5] Matsumoto T., Matsumoto H., Yamada K., Hoshino S., "Impact of Artificial "Gummy" Fingers on Fingerprint Systems", in *Proc. SPIE*, pp. 275-289, 2002.
- [6] Putte T.v.D., Keuning J., "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned", in *Proc. Working Conference on Smart Card Research and Advanced Applications*, pp. 289-303, 2000.
- [7] Schuckers S.A.C., "Spoofing and anti-spoofing measures", *Information Security Technical Report*, vol. 7, pp. 56-62, 2002.