ISSN 1726-5479

# SENSORS & TRANSDUCERS

vol. 136
1 /12

## Sensor Instrumentation, DAQ and Virtual Instruments

International Frequency Sensor Association Publishing

IFSA

# Sensors & Transducers

Volume 136, Issue 1
January 2012

www.sensorsportal.com

ISSN 1726-5479

Sensors & Transducers Journal (ISSN 1726-5479) is a peer review international journal published monthly online by International Frequency Sensor Association (IFSA).
Available in electronic and on CD. 

**Sensors & Transducers Journal**

# Contents

**Volume 136**
**Issue 1**
**January 2012**

**www.sensorsportal.com**

**ISSN 1726-5479**

## Research Articles

**Digital Sensors and Sensor Systems: Practical Design**
*Book Review*……………………………………………………………………………………………….. I

**Fast and Simple Measurement of Position Changes**
*White Paper, iC-Haus GmbH*…………………………………………………………………………….. IV

**A Novel Method of Linearizing Thermistor Characteristic Using Voltage Controlled Oscillator**
*Narayana K. V. L and Bhujanga Rao A.*............................................................................... 1

**A Data Acquisition System Based on DSP for Mechanical Nanoscale Displacement Sensor**
*Yong Yu, Qian Wu, Hanyu Sun, Zhengwei Li and Yunjian Ge* ......................................................... 12

**Modified AC Wheatstone Bridge Network for Accurate Measurement of Pressure Using Strain Gauge Type Pressure Sensor**
*Subrata Chattopadhyay, Mahuya Banerjee and Sagarika Pal*.......................................................... 25

**Fingerprint Sensors: Liveness Detection Issue and Hardware based Solutions**
*Shahzad Memon, Nadarajah Manivannan, Azad Noor, Wamadeva Balachadran, Nikolaos V. Boulgouris* ......................................................................................................... 35

**Fiber Optic Vibration Sensor Using Pmma Fiber for Real Time Monitoring**
*P. Kishore, D. Dinakar , D. Sen Gupta, P. Saidi Reddy, M. Sai Shankar, K. Srimannarayana* ......... 50

**ARM Processor Based Multisensor System Design for the Measurement of Environmental Parameters**
*NarasimhaMurthy Yayavaram, Soundara Rajan, Vishnu Vardhan*.................................................... 59

**A Decoupling Algorithm Based on Homotopy Theory for 3-D Tactile Sensor Arrays**
*Junxiang Ding, Yunjian Ge, Yuan Wang, Zhaohui Wang* .................................................................. 72

**Digital Imaging and Piezo-dispenser Actuator in Automatic Flocculation Control**
*Jani Tomperi, Markus Honkanen, Pasi Kallio, Kauko Leiviskä, Pentti Saarenrinne, Iiris Joensuu, Marjatta Piironen* ......................................................................................................... 83

**An Embedded Web based Real Time Application for Remote Monitoring & Controlling of MST RADAR Transmitters**
*Nagabhushan Raju Konduru, Lakshmi Narayana Roshanna, Rajendra Prasad Thommundru, Chandrasekhar Reddy Devanna*......................................................................................... 96

**Advanced Oscilloscope Triggering Based on Signal Frequency**
*Shakeb A. Khan, Alka Nigam, A. K. Agarwala, Mini S. Thomas, T. Islam* 105

**Pyramidal Traceability Hierarchy for Pressure Measurements and Calibrations at NIS- Egypt**
*A. A. Eltawil*......................................................................................................................... 118

**Fuzzy Logic Based Autonomous Traffic Control System**
*Muhammad Abbas, M. Saleem Khan, Nasir Ali and Syed Fazil* ........................................................ 132

**Potential of Piezoelectric Sensors in Bio-signal Acquisition**
*Dipali Bansal*......................................................................................................................... 147

**Measurement and Analysis of Sodium in Vegetables Using ATmega16 Microcontroller Based Spectrophotometer**
*K. Murugananthan and P. Neelamegam..* ........................................................................... 158

Authors are encouraged to submit article in MS Word (doc) and Acrobat (pdf) formats by e-mail: editor@sensorsportal.com
Please visit journal’s webpage with preparation instructions: http://www.sensorsportal.com/HTML/DIGEST/Submition.htm

International Frequency Sensor Association (IFSA).


*Sensors & Transducers Journal, Vol. 136, Issue 1, January 2012, pp. 35-49*

**Sensors & Transducers**

**ISSN 1726-5479**

*http://www.sensorsportal.com*

# Fingerprint Sensors: Liveness Detection Issue and Hardware based Solutions

**Shahzad Memon, Nadarajah Manivannan, Azad Noor, [1] Wamadeva Balachadran, [2] Nikolaos V. Boulgouris**
Centre for Electronic System Research (CESR),
Electronics and Computer Engineering, School of Engineering and Design, Brunel University,
London, UK
[1]Tel: +44 (0)1895 265774, fax: +44 (0)1895 258728
Tel: +44 (0)1895 267629, fax: +44 (0)1895 258728
E-mail: shahzad.memon@brunel.ac.uk, nadarajah.manivannan@brunel.ac.uk,
azad.noor@brunel.ac.uk, wamdava.balachanderan@brunel.ac.uk, nikolaos.boulgouris@brunel.ac.uk

*Received: 27 October 2011 /Accepted: 24 January 2012 /Published: 30 January 2012*

**Abstract:** Securing an automated and unsupervised fingerprint recognition system is one of the most critical and challenging tasks in government and commercial applications. In these systems, the detection of liveness of a finger placed on a fingerprint sensor is a major issue that needs to be addressed in order to ensure the credibility of the system. The main focus of this paper is to review the existing fingerprint sensing technologies in terms of liveness detection and discusses hardware based 'liveness detection' techniques reported in the literature for automatic fingerprint biometrics.


**Keywords:** Fingerprint Sensors, artificial fingers, spoofing, Liveness.

## 1. Introduction

The use of fingerprint for a biometric identification is one of the most prevalent authentication methods used today in a number of commercial, civil and forensic applications. In the last decade, research in fingerprint based identification systems has reached to a higher degree of accuracy [1-3], [4]. The academic and industrial research in fingerprint biometric has achieved more maturity than other biometric systems and it almost becomes the synonym for biometric systems. Automatic Fingerprint

Biometrics is now an accepted system for securing commercial and homeland security systems. In the past few years, many hardware and software technologies have been tested for capturing, storing, processing and matching fingerprint data. The main reasons for the success and proliferation of this technology are: wider acceptance of fingerprints as a biometric means and availability of low-cost fingerprint acquisition devices. In spite of their numerous advantages, recent research has pointed out that the current fingerprint sensing technology can be deceived by a fake or artificial fingerprint made of gelatine or similar kind of materials [5-7]. Many believe that fingerprint biometric systems can detect liveness in biometric samples, however; artificial fingerprints created today are close to the original real finger, and it has been proved that about 80%-85% of these systems are easily fooled by different kinds of fake fingers with stamped patterns. Therefore, the issue of 'Liveness Detection' has emerged in biometrics research. Liveness detection refers to the inspection of the characteristics of a finger in order to check whether the input finger is live or artificial. Currently, a number of fingerprint identification systems are being used and implemented at various important places such as airport, border and immigration controls. However, in most cases, the ability to detect liveness does not appear to be a major concern of the manufacturers of these systems. The possible measures to detect liveness are only proposed in patents and published literature. In January 2009, a woman at Tokyo airport managed to fool a fingerprint reading machine by using a piece of tape stuck on her fingers. Japanese officials said in a report that they suspected many others had been doing the same things, demonstrating that the biometric systems they installed in 30 airports in 2007 at a cost of $45 million are completely useless [8]. This incident has made it clear that there is no known fingerprint biometric hardware or software solution that is 100 % fool-proof. Various liveness detection methods proposed in literature are to possibly implement either at the acquisition stage or at the processing stage. It is extremely difficult to identify these fake fingers simply via image processing algorithms. There should be new sensing technology/or some kind of extended hardware, that can differentiate living tissues from artificially created materials resembling it.

This paper is divided into five sections. Section one introduces the spoofing issue with fingerprint biometrics; section 2 discusses the details of fingerprint sensor technologies. Fingerprint sensing technologies are explained in section 3. Proposed hardware based liveness detection techniques are described in section 4. The conclusions are drawn in section 5.

## 2. Spoofing Techniques in Fingerprint Sensors

Before describing spoofing in more detail, it may be helpful to discuss how the False Acceptance Ratio (FAR), a typical efficiency measure of biometric devices, is related to spoofing. A false-accept occurs when a submitted template is incorrectly matched to a template enrolled by another user [1, 9]. This only refers to a zero effort attempt, i.e., an unauthorized user making an attempt with his/her own biometric to gain access to a system. If the FAR is kept low, then the probability of specific user with criminal intent matching another template is very low. The FAR does not give information on the vulnerability of a system to spoof attacks.

The fraudulent entry of an unauthorized person into a fingerprint recognition system by using fake fingerprint sample is termed spoofing. The spoofing of fingerprint sensors was first revealed by Network Computing in 1998 [5]. They addressed the vulnerability of fingerprint scanning devices by testing with fake/lifted fingerprints; resulting four out of six devices were susceptible to fake finger attacks. Further research was undertaken by Tsutomu Matsumoto to prepare fake fingerprint stamps using low-cost, easily obtainable tools and materials such as silicon and Gelatine (Fig. 1. Method-1& 2). The images produced by these fake fingers were accepted as a real finger tips by 11 types of fingerprint systems (Fig. 1: Fingerprint) [10].

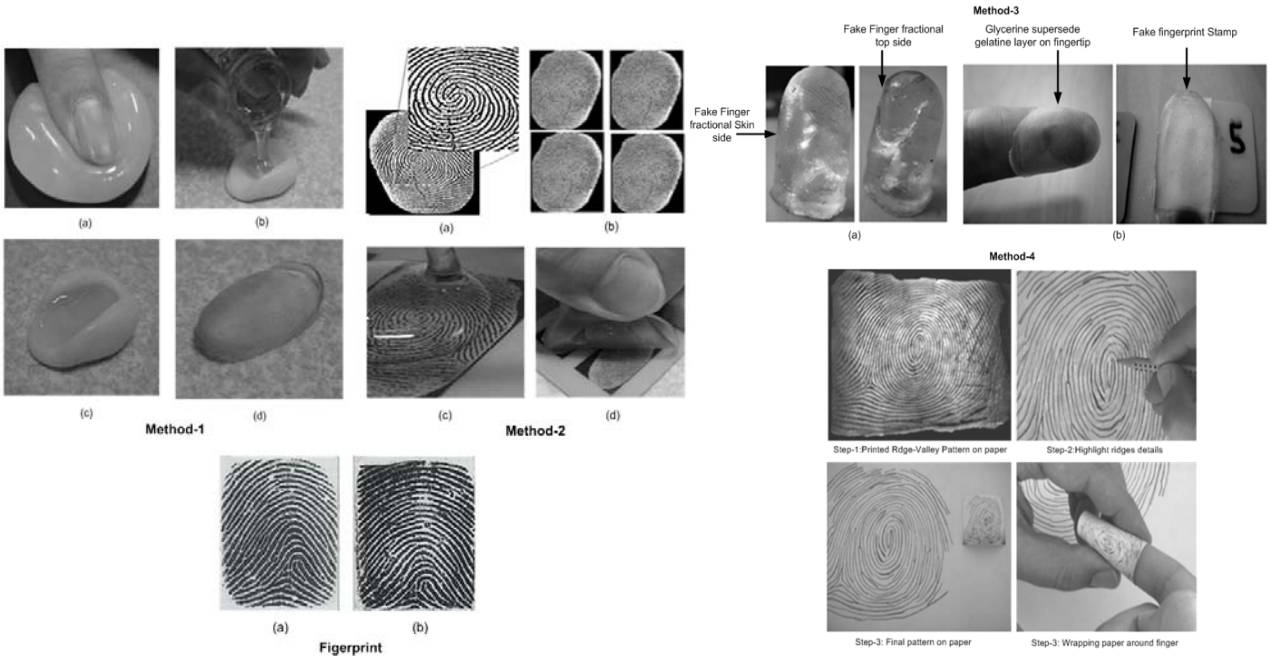



**Fig. 1. Method-1**: Process of making fake fingerprint from plastic/ silicon mould a) Pressing of finger on soft plastic silicon/rubber mould b) Dripping of liquid gelatine/rubber over mould c) Solidification d) Artificial fingerprint stamp [10].**Method-2** a) Imaging of fingerprint from residual fingerprint b) Making and printing of fingerprint c) Masking and printing of fingerprint d) Detaching of fake fingerprint stamp [6, 10], Method-3: GSG based fake finger and fingerprint (a) Glycerine based 3-D fake finger (b) Finger sample [11] Method-4: Four step fake fingerprint preparation to spoof the touchless surrounded biometric system.[12]**. Fingerprint:** a) Live Finger b) Fake/Gummy Finger [6].

In many tests, it has been shown that high FAR with optical/ capacitive fingerprint sensors. In these test, fake finger- print enrolment achieved with 68–100% acceptance [6, 10], [7], [13].

In August 2003, two German hackers claimed to have developed a technique using latent prints on the scanner and convert them to a latex fingerprint [14]. They used graphite powder and adhesive tape to recover the latent prints that were digitally photographed, and then enhanced by using graphics software. Recent publication [11] has explained some new techniques of making 3D fake fingers (Fig. Method-3 a) and fingerprint using materials such as Glycerine Supersede Gelatine (GSG) shown in Fig. 1 Method 3. b). The GSG based fake fingers have been tested on capacitive, optical and thermal sensors and they have been successfully enrolled and matched.

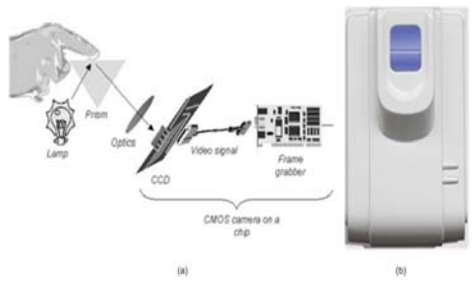
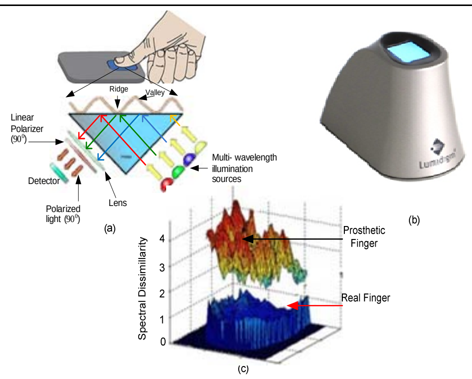
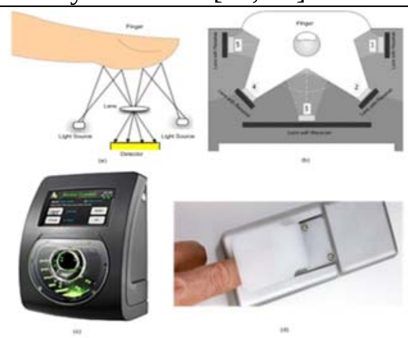
Touchless surrounded imaging based fingerprint technique is also spoofed with a piece of paper containing print of ridges and valley pattern of finger. The four step procedure of preparing fake fingerprint sample for touchless surrounded imaging is illustrated in Fig. 2 Method-4.

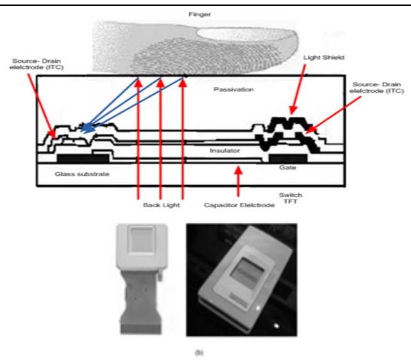
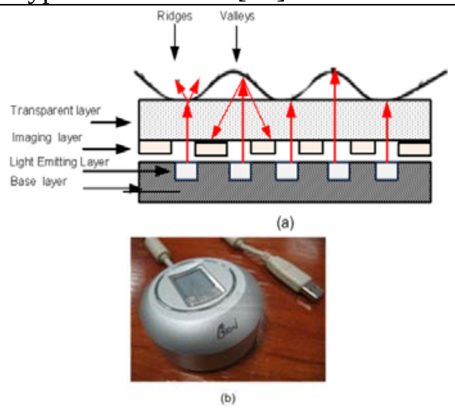
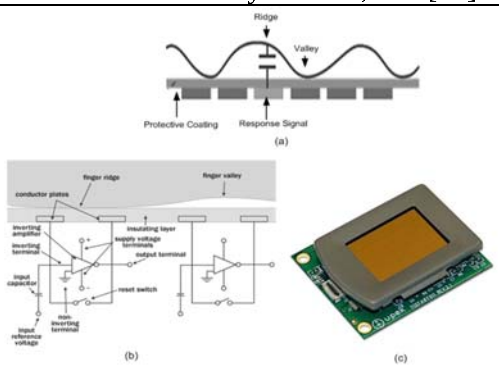
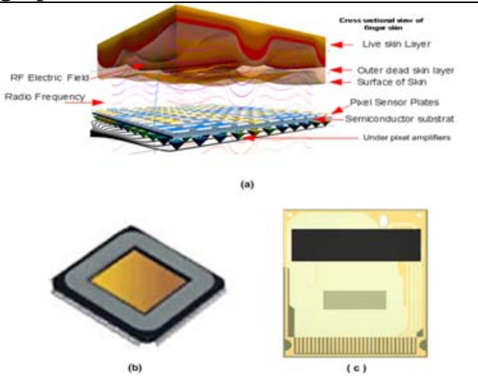
Much of the activity in spoofing biometric systems has, up until now, been confined to researchers. Moreover, as biometric systems become more widespread, the incentives to misuse or hack biometric systems will grow. Understanding the nature and risk of such attacks will become increasingly important to systems architects, administrators and systems security managers.

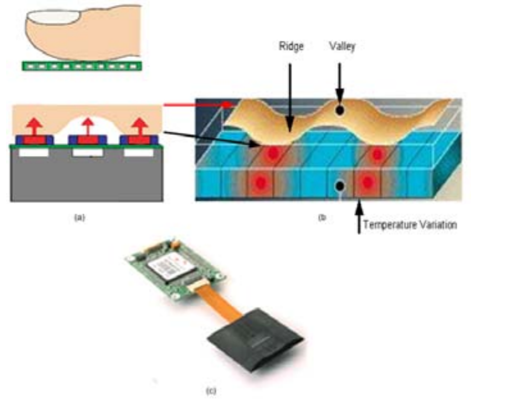
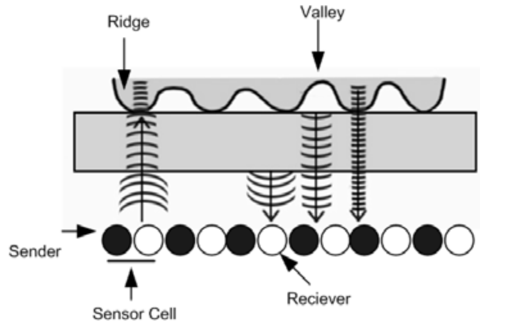
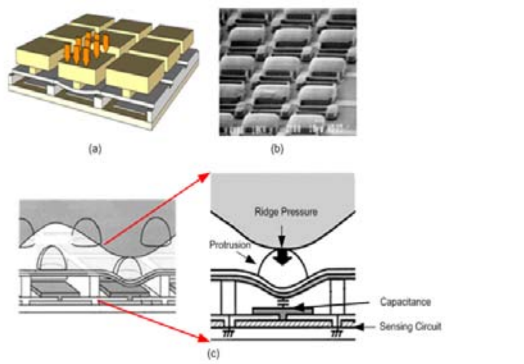
## 3. Fingerprint Sensing Technologies

Fingerprint sensor is the most important part of a fingerprint scanner where the image is formed. Many sensing technologies have been evolved over the past few years such as optical, electro-optical, capacitive, piezoelectric, thermal , ultrasound and radio frequency. In the following section, major fingerpint sensing techniques are illustarted with their advantages and dissdvantages in Table 1.

**Table 1.** Fingerprint Sensing Technologies.

| Technology | Sensing Principle | Advantages and Disadvantages |
|---|---|---|
| **Optical**<br>**Frustrated Total Internal Reflection (FTIR)** | <br>(a) FTIR Mechanism [15] b) MIAXIS FPR-620Optical fingerprint reader [16] | • High resolution (500-1200 PPI)<br>• Less sensitive to mechanical shocks or Electro-Static Discharge (ESD).<br>• Very suspectable to non-ideal skin conditions, in particular, if the skin is too dry or not in good contact with the sensor<br>• Cannot distinguish between fake and original fingerprints. |
| **Multi-Spectral Imaging** | <br>(a) Principle of Multispectral Fingerprint Imaging (b) lumidigm Mercury SeriesM301multispectral imaging technology based Fingerprint Reader.[17](c) Spectral dissimilarity test result [18, 19] | • Combination of surface and subsurface imaging<br>• Cable to collect more identifying data from the finger<br>• Insensitive to adverse environmental effects such as mechanical shocks or ESD<br>• Decieved by the use of fake fingers created with silicon and thermoplastic matirials. |
| **3D Touch-less Imaging** | <br>(a) Principle of Toucless Fingerprint Imaging [20] (b) Touchless finegrprint scanner with five optical sou<br>(b) rces and detect [12] (c) TBS 3DGuard Touchless fingerprint scanning Terminals [21] (d) FlashScan 3D touchless fingerprint reader [22] | • Remote sensing technique used to capture the ridge-valley patterns with no contact between the skin of the finger and the sensing area.<br>• Capture of a full nail-to nail fingerprint<br>• Expensive technique compared to other technologies<br>• Lower image contrast, illumination, correct finger positioning and user convenience.<br>• It is not fool proof |

| | | |
|---|---|---|
| **Thin Film Transistor (TFT)** | <br>( a) Schemetic of TFT Optical type fingerprint sensor (b) Two optical TFT prototype from CASIO [15] | • Compact and low power consumption<br>• TFT based fingerprint sensors could be a useful solution to integrate within touch display<br>• There is no liveness detection included yet in the TFT sensor |
| **Electro-optical** | <br>(a) Sensing principle of Electro-optical fingerprint [23] (b) Bio-i CYTE fingerprint sensor manufactured by Testech, Inc. [24] | • Compact and low power consumption<br>• No liveness test reported with this technology |
| **Other**<br>**Capacitive** | <br>(a) Capacitive Fingerprint Sensing mechanism (b) Capacitance detection circuit [25] ( c) UPEK's TCS1 TouchChip Fingerprint Sensor [26] | • Commonly available and economical<br>• Dielectric constant of the surface layer is mainly due to moisture in the dead cells, ridges in dry fingers will have dielectric constants very close to air, resulting in very faded images<br>• vulnerable to strong external electrical fields, the most detrimental being ESD<br>• Failed in various liveness detection tests and were easily spoofed with fake finger stamps |
| **Radio Frequency (RF)** | <br>(a) Principal of RF field sensing [23] b) Authentic AES 4000 [27]<br>(c) Valadity Liveflex VFS 201 Sensor [28] | • RF based technique detect subsurface (live layer) of fingertip.<br>• Fingerprints that are difficult or impossible to acquire using capacitive sensors can be successfully acquired with RF Technology<br>• A gummy finger can still successfully fool the scanner because the conductance of a properly made gummy finger is almost similar to that of a real live finger |

<table>
<tr>
<td>Thermal</td>
<td><br>(a) Cross sectional view of a thermal fingerprint sensor [29] (b) Sensing mechanism [15] (c) Atmel AT77C104B FingerChip™ Swipe fingerprint sensor [30]</td>
<td>• It only scans surface skin of fingertip by measuring the heat transferred from the sensor array to fingertip<br>• It operate well under extreme temperatures, high humidity, oil and dirt<br>• Heating of the sensor array increases the power consumption<br>• Also incapable to differentiate between fake and live finger tip</td>
</tr>
<tr>
<td>Ultrasound</td>
<td><br>Principles of ultrasound fingerprint sensing [23]</td>
<td>• Can read the sub-surface of the skin rather than the surface only<br>• Tolerant to ambient light, humidity, extreme temperatures and ESD.<br>• Takes couple of seconds to generate the image<br>• Big size and higher cost<br>• Poor image quality and susceptible to spoofing</td>
</tr>
<tr>
<td>Micro-Electro-Mechanical Systems (MEMS)</td>
<td><br>a) 3D view of MEMS fingerprint sensor [31]<br>b) SEM Images of MEMS fingerprint sensor [15]<br>c) Principle of MEMS fingerprint sensors [32, 33]</td>
<td>• An array of tiny silicon switches<br>• Direct binary output<br>• Significant characteristics such as durability, low power consumption, being resistant to ESD, non bulky in shape<br>• No further development has been reported with this technique beyond the laboratory<br>• No liveness test on has been reported in literature yet</td>
</tr>
</table>

## 4. Proposed Hardware based Liveness Detection Methods

Liveness detection for fingerprint scanners can be achieved by adding extra hardware to acquire liveness signs. Human body offers a vast amount of various characteristic, but not all of them comply with foregoing requirements and not all of them can be used with the fingerprint technology. For the liveness detection systems, the usable properties of human body can be split into three categories such as intrinsic physiological properties, Biological or involuntarily generated signals and responses to a stimulus. The reported hardware based liveness detection techniques are classified and illustrated in Fig. 2.

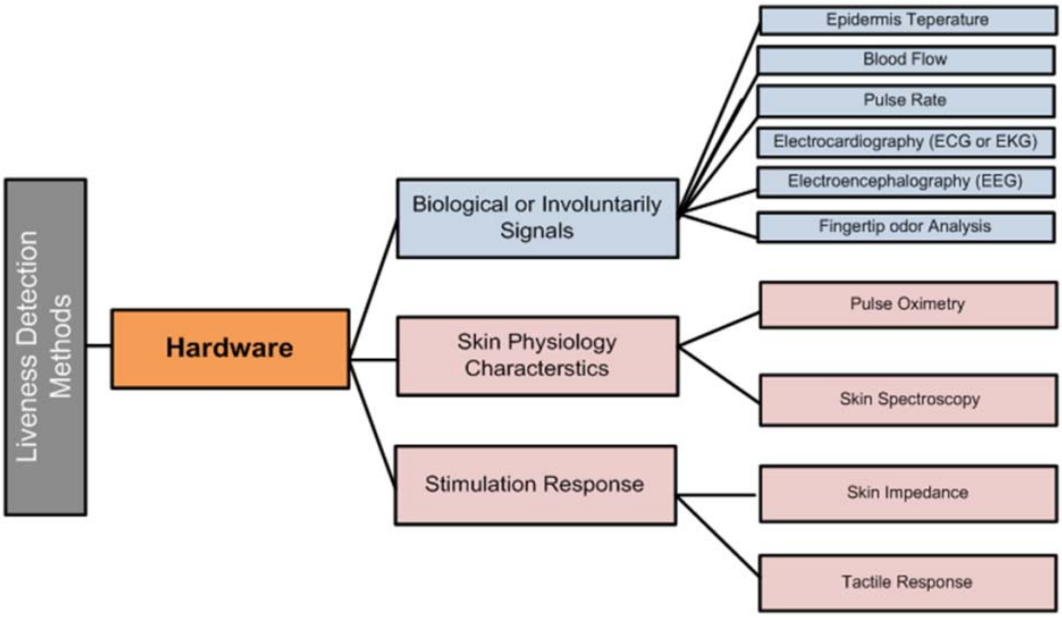



**Fig. 2.** Classification of Hardware based Liveness Detection Methods.

Measurement of biological signals to detect liveness of the fingertip placed on the surface of the sensor are obviously expensive approach as they require additional hardware and can be strongly invasive: for example, measuring person's blood pressure can be used for other reasons than for simply detecting the liveness of his/her fingertip.

### 4.1. Biological Signals

A living human body generates many bio signals that can be observed from the many measuring points available on the surface of the body. Some of the bio signals can be detected and measured from the tip of the finger of a person. Most of the hardware based liveness detection techniques recommended in literature uses the biomedical sensors to measure the continuation of bio signals to verify the liveness. The following techniques were suggested from different researchers to overcome the liveness issue in fingerprint sensors.

#### 4.1.1. Blood Flow

In 1998, a US patent entitled "Anti-Fraud Biometric Sensor" that accurately detects blood flow by Smart Touch LLC [34] describes the method of blood flow detection in finger. This method uses two light emitting diodes (LEDs) and a photo-detector used to determine whether blood is flowing through the finger. Furthermore; this patent declares to have solved these problems by checking if the background light level is above a threshold and by detecting movement of the finger. However; similar solutions have been possible to fool by simulating blood flow through the use of a flashing light or by moving the imposters' finger.

#### 4.1.2. Pulse Rate

In this method the underlying finger's pulse will be sensed. However; practical problems arise due to changes in the pulse. Suppose, a person with a pulse of 30 beats per minute implicates that the finger must be held for at least few seconds on the sensor for the pulse to be detectable. However, the pulse rate is also affected by emotional states and the same person could have a pulse rate more than 30 beats per minute if he or she worked out immediately before the fingerprint scanning and this needs an extra sensor and processing with fingerprint hardware.

#### 4.1.3. Electrocardiography (ECG or EKG)

The contraction and relaxation of cardiac muscle result from the depolarisation and repolarisation of myocardial cells. These electrical changes are recorded via electrodes placed on the limbs and chest wall and are transcribed on to a graph paper to produce an electrocardiogram (commonly known as an ECG) [35, 36]. However, the measurement of ECG pulses is easily fooled with a small signal generator and unrealistic with access to only one fingertip. In addition, the implementation of this system with fingerprint sensor requires expensive hardware and processing costs.

#### 4.1.4. Electroencephalography (EEG)

An EEG is a painless test that records brain activity. When the brain cells send messages to each other they produce tiny electrical signals [37]. The EEG signals are recorded from the subject while being exposed to a stimulus, which consist of drawings of objects chosen from Snodgrass and Vanderwart picture set [38]. However, the measurement of EEG-pulse is easily fooled with a small signal generator. Furthermore, it is unrealistic to use EEG with only access to one fingertip.

#### 4.1.5. Finger Skin Odour Analysis

This method is based on the acquisition of the odour by means of an electronic nose, whose response in presence of human skin differs from that obtained in the presence of other materials [39], usually employed to fake fingerprints. An odour sensor is used to sample the odour signal and an algorithm allows discriminating the finger skin odour from that of other materials such as latex, silicone or gelatine, usually employed to forge fake fingerprints [39, 40], [59, 60]. The acquisition of an odour pattern consists of sampling the data coming from sensor during a given time interval; usually few seconds. The limit of this method is time necessary to restore the sensor response. It may vary on the sensor characteristic and environmental condition. In addition, experimental results confirm that this method, which is able to effectively discriminate real fingerprints from fake, can be forged using a wide range of materials.

#### 4.1.6. Temperature of Finger Tip Epidermis

Temperature is an involuntarily generated signal under the finger tip. It is quite easy to measure it, but not sufficient to detect liveness. Average temperature on fingertips ranges between 26 °C and 30 °C [41], [42]. However, the temperature depends on the health condition of the user (fever or poor blood circulation could influence the result of the liveness detection). This could make an impostor with a thin artificial fingerprint attached on his real finger be accepted and, on the other hand, a user with poor blood circulation or cold be rejected. If a thin silicon artificial fingerprint is patched on a real finger, the temperature can be decreased by a maximum of 2 $^0$C, which is well inside the working margins of the sensor. Sensors that are used outdoors often have a broader working margin, giving the intruder even more chance.

### 4.2. Skin Physiology Characteristics

Human fingers are known to display friction ridge skin that consists of a series of ridges and furrows, generally referred to as fingerprints (Fig. 3 a, b & c). The friction ridge skin is made of two major layers: dermis (inner layer) and epidermis (outer layer), as shown in Fig. 3 d & e.

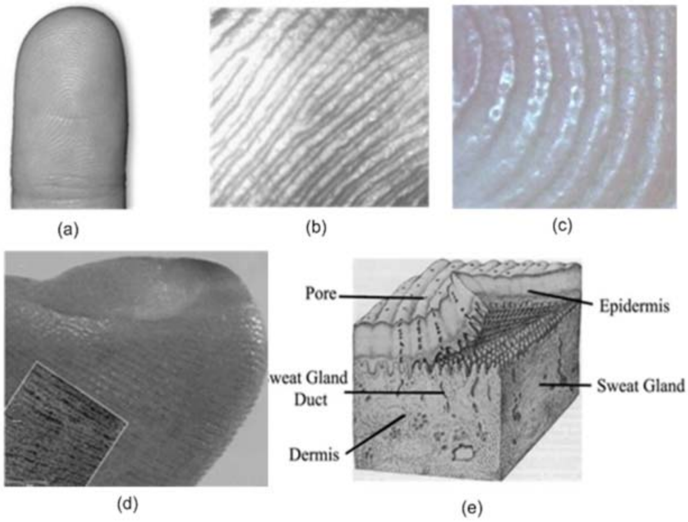



**Fig. 3.** a) Finger Tip, b) friction ridge skin, c) Sweat pores on ridges, d) The epidermis is partly lifted from the dermis, e) A three-dimensional representation of the structure of ridged skin [43].

A typical young male has, on an average, 20.7 ridges per centimeter while a female has 23.4 ridges per centimeter [43]. It is suggested that friction ridges are composed of small "ridge units," each with a pore, and the number of ridge units and their locations on the ridge are randomly established. As a result, the shape, size, alignment of ridge units, and their fusion with an adjacent ridge unit are unique for each person (Fig. 3 a & c). Although, some cases exist where ridge units fail to compose a ridge, also known as dysplasia, independent ridge units still exist on the skin.

#### 4.2.1. Pulse Oximetry

Pulse oximetry is used in the medical field to measure the oxygen saturation of haemoglobin in a patient's arterial blood [44] . In this method the pulse and blood oxygenation are measured by shining the beams of light through the finger tissue (Fig. 4).

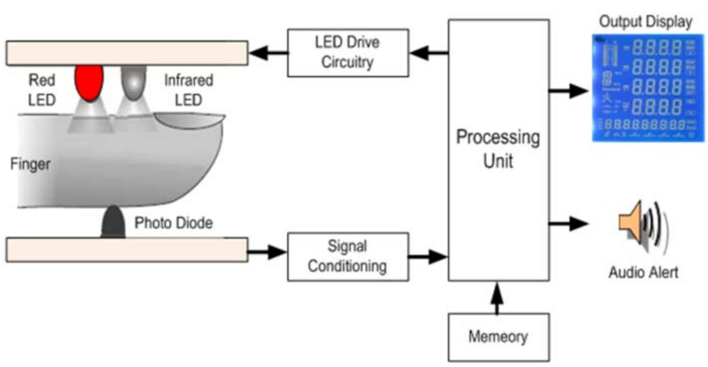



**Fig. 4.** Pulse Oximatery Technique.

The oxygenated haemoglobin allows red light to transmit through and absorbs more infrared light while the deoxygenated haemoglobin allows infrared to transmit through and absorbs more red light. Usually, a finger is placed between the source (LEDs) and the receiver (photodiode) acts as a translucent site with good blood flow. Once these absorption levels are detected from the finger, the ratio of absorption at different wavelengths can be obtained.

The advantage of this method, inherent in its origin, is the well known principle of pulse oximetry, which is especially used in medicine; however, it takes long time for scanning pulses and possibly the measurements will fail in cold weather because of the lack of microcirculation in the fingertip. In addition, it can easily circumvent with the use of a thin fake finger layer made using gelatine.

### 4.2.2. Skin Spectroscopy

In skin spectroscopy, optical technique is used to measure the absorption of light by tissue, fat, blood and melanin pigment. This measurement system is based on optical source that illuminates a small area of fingertip skin with multiple wavelengths of visible and infrared light as shown in Fig. 5.

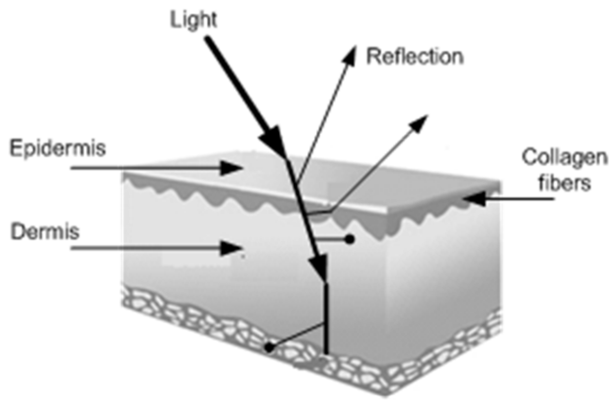



**Fig. 5.** Skin Spectrometry.

Light undergoes scattering and absorption at different layers of skin. Scattering is caused by the structural characteristics such as the arrangement of the collagen fibers and absorption is caused by chromophores in the layers. The depth of light penetration depends on the wavelength of the light and the level of pigmentation. The light is reflected back after being scattered in the skin and is then measured for each of the wavelengths. The system analyzes the reflectance variability of the various wavelengths such as, 400–700 nm as they pass through the skin. Because the optical signal is affected by chemicals and other changes to the skin, skin spectroscopy also provides a sensitive and relatively easy way to confirm that a sample is living tissue [45], [46]. Furthermore, the reflectance spectrum of skin provides information regarding the distribution and concentration of various chromophores present in the skin and is highly dependent on the person's physical characteristics. Thus spectroscopic measurements can be successfully used as a biometric. However, the system needs a moderate environmental conditions and it might slow the access control process.

### 4.3. Stimulus Response

The stimulus response of the skin can be obtained by applying small external electrical signals and measuring the variation.

### 4.3.1. Skin Impedance

The skin impedance method is based on simultaneous measurements of the electrical bio impedance of different skin layers. The measurements are sensitive to skin properties like stratum corneum impedance and viable skin impedance. Dispersive behaviour of these layers can be detected in the measured frequency range and anisotropy in the stratum corneum [47].

The electrical impedance measurement system is illustrated in Fig. 6. This system uses electrode array with three alternative current injecting electrode sets and one set of voltage pick-up electrodes. The two middle electrodes are connected to the differential voltage input of the frequency response analyzer, and the other three electrode pairs (denoted as $i_1$, $i_2$, $i_3$ in Fig. 6) were in turn connected to the internal oscillator. The frequency response analyzer consequently performed three successive four-electrode measurements, each time using the same voltage pick-up electrodes, but different current injecting electrode pairs (denoted as inner, middle and outer in Fig. 6). In each measurement, a live or fake finger placed on the top of the electrode system with a light pressure and then three frequencies scan were performed using an applied voltage on the current injecting electrodes with discrete frequencies.

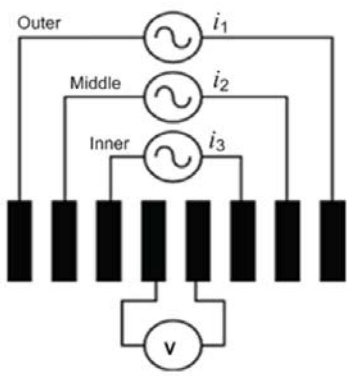



**Fig. 6.** Electrical Impedance Measurement System [47].

The sensitivity field of a four-electrode system is found by taking the dot product of the current density vectors resulting from driving a unity current through the current injecting electrodes and voltage pick-up electrodes, respectively [47]. Up till now, this system is tested at prototype level and proposed as a liveness detection solution for fingerprints sensor modules. However; it is not tested or implemented with actual fingerprint modules.

### 4.3.2. Eleltrotactile

The theory behind the electrotactile stimulation is the understanding of human touch sensation. The live skin is sensitive to temperature, vibrations, pressure, electrical voltage and current, with different receptors located at different depth of the skin for each sensation. Such tactile perception capability is absent in fake or dead skin. Eletcrotactile method uses electrical means to directly activate the nerve to stimulate the sense of touch. Such tactile system typically involves a matrix of surface electrodes that pervade very small, controlled electric currents into skin (Fig. 7).

Liveness detection method based on electrical based tactile sensation is proposed in [48]. This system is capable of presenting tactile pattern of fake and live finger tip skin. The initial results from prototype shows that the proposed approach is indeed able to detect gelatine fake finger worn over live fingers, even when the gelatine is only 1mm thick. The only uncertainty is whether a finger with a thin fake layer such as those made using gelatine, can still provide the person with sufficient touch perception to circumvent the system.

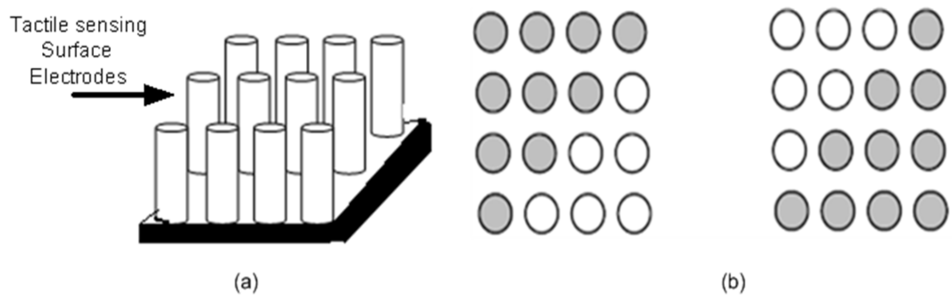



**Fig. 7.** a) 3D representation of Electrotactile Electrode Array b) A 4-by-4 electrode pad showing an upper triangular (left) and lower triangular (right) tactile pattern. Each circle is an electrode. The dark circle represents an active electrode (having current flow) while the light circle represents an inactive electrode [48].

The following table summarizes the requirements and limitations of hardware based liveness detection methods discussed in the above sections.

**Table 2.** Summary of Hardware based Liveness Detection Techniques.

| Methods | Liveness Detection Technique | Requirements | Limitations |
|---|---|---|---|
| **Biological Signals** | Epidermis Temperature | Additional Temperature sensing and signal processing hardware | • Measurement Time and cost |
| | Blood Flow<br>Electrocardiogram (ECG) | Biomedical sensors and signal processing hardware | • Setup for measuring the noise free bio signals<br>• Interface with fingerprint sensor<br>• Cost and size issues |
| | Electroencephalogram (EEG) | Detection Electrodes | • Easily fooled (with a small signal generator)<br>• Impractical with access to only one fingertip |
| | Pulse Rate Detection | Optical Sensors and measurement systems | • Environmental conditions<br>• Size and cost of hardware<br>• Integration with fingerprint scanners |
| | Odor Analysis | Sensors to detect different type of odor | • Extra sensors<br>• Detection timing and Processing<br>• Cost and system size |
| **Skin Physiological Characteristics** | Pulse oximetry | Optical sensors | • Biomedical hardware requirement<br>• Complex signal processing |
| | Skin spectroscopy | • Different Optical sources and sensors<br>• Additional measurement Systems | • Size of system<br>• Additional signal processing and software requirements<br>• Not feasible in mobile applications |
| | Skin Impedance | • Electrodes Array<br>• External Dc Voltage | • Skin condition can change resistance<br>• Additional power |
| | Eleltrotactile | • Array of Electrodes with additional measurement system | • Deign of electrode array and size<br>• Addition Signal processing hardware Integration of fingerprint sensors |

The design, cost, user acceptance and implementation are common issues with the proposed hardware based liveness detection solutions. It needs more research and investigation to find a suitable solution that can bring the balance among price, user-friendliness and security of the system.

## 5. Conclusion

To discourage possible attackers from presenting a fake finger using artificial methods, it is important to ensure that the finger presented to the sensor is genuine and it is not a fake/artificial or from a cadaver. Consequently, a live finger detection mechanism is a crucial part of any fingerprint identification system used for security reasons. In any practical fingerprint acquisition system, the live finger detection should be performed simultaneously with the capture of the fingerprint which seems unlikely with currently available fingerprint technologies without additional hardware. The only possibility is to redesign the fingerprint sensing technology that will be able to detect liveness from placed finger without addition of extra hardware.

For liveness detection in fingerprint sensor, it is necessary to choose a property of fingertip, which is difficult or impossible to imitate. The chosen liveness detection method should be easy to implement as a hardware or software solution, so that the final price of such security solution would be not too high. Among many possible techniques for liveness detection from fingertip, an elegant method is to sense ionic activities in sweat pores present on fingertip ridges. The authors of this paper are investigating the novel liveness detection method on a fingertip using nanotubes/nanowires based sensor by detecting ionic activities from sweat pores. The findings of this research will be used to characterize a novel nanotechnology based fingerprint sensor which might help to reduce the FAR and FRR and lead the design of such a sensor with inherent features of liveness detection.

## References

[1]. Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S. Handbook of Fingerprint Recognition, *Spinger*, 2009.
[2]. D. Maltoni and R. Cappelli, Advances in fingerprint modeling, *Image Vision Comput.*, Vol. 27, 2/2, 2009, pp. 258-268.
[3]. S. S. Adebisi, Fingerprint Studies - The Recent Challenges and Advancements: A Literary View, *The Internet Journal of Biological Anthropology*, Vol. 2, 2009, pp. 1-15.
[4]. A. Abhyankar and S. Schuckers, Integrating a wavelet based perspiration liveness check with fingerprint recognition, *Pattern Recognit*, Vol. 42, 3, 2009, pp. 452-464.
[5]. W. David, L. Mike, Six biometric devices point the finger at security. [Online]. 2010 (03/05), pp. 2, 2010, Available: http://www.networkcomputing.com/910/910r1.html
[6]. T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, Impact of artificial fingers on fingerprint systems, *Proceedings of SPIE*, San Jose, CA, USA, Vol. 4677, 2002, pp. 275-289.
[7]. S. A. C. Schuckers, Spoofing and Anti-Spoofing Measures, *Information Security Technical Report*, Vol. 7, 12, 2002, pp. 56-62.
[8]. Y. Flink. Million dollar border security machines fooled with ten cent tape. Find Biometrics-Global Identity Management [Online]. 2010 (03/13), 2009, Available: http://www.findbiometrics.com/articles/i/6090/
[9]. D. Petrovska-Delacrétaz, G. Chollet, K. Anil and B. Dorizzi, Guide to Biometric Reference Systems and Performance Evaluation, *Springer-Verlag*, New York Inc, 2009.
[10]. T. Matsumoto, Gummy and Conductive Silicone Rubber Fingers Importance of Vulnerability Analysis, *Advances in Cryptology—ASIACRYPT*, 2002, pp. 59-65.
[11]. C. Barral and A. Tria, Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin, *Formal to Practical Security*, 2009, pp. 57-69.
[12]. M. Tistarelli, S. Z. Li and R. Chellappa, Handbook of Remote Biometrics: for Surveillance and Security, *Advances in Pattern Recognition*, 2009, pp. 382.

[13].U. Uludag and A. K. Jain, Attacks on biometric systems: A case study in fingerprints, *in Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents*, VI, 2004, pp. 622-633.
[14].C. Roberts, Biometric attack vectors and defences, *Comput. Secur.*, Vol. 26, 2, 2007, pp. 14-25.
[15].Jean-François Mainguet, Fingerprint sensors, [Online] 2010 (03/12), 2009, Available: http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_sensors_productsi.htm
[16].L. MIAXIS Biometrics Co, FPR-620 Optical Fingerprint Reader, Vol. 2010, 2009.
[17].I. Lumidigm, Mercury desktop sensor, [Online] 2010 (8/10), Available: http://www.lumidigm.com
[18].Lumidigm Inc., Liveness detection, [Online] 2010 (03/13), 2010. Avalable: http://www.lumidigm.com/liveness-detection/.
[19].K. Nixon and R. Rowe, Spoof detection using multispectral fingerprint imaging without enrollment, *in Proceedings of Biometrics Symposium (BSYM2005)*, Arlington, VA, 2005.
[20].Fingersys, *Fingerprint Biometrics*, Vol. 2010, pp. 08.
[21].TBS inc. Touchless terminals- the TBS 3D guard series, [Online]. 2010(8/13), Available: http://www.tbsinc.com
[22].Flash Scan3D, 3D Touchless Fingerprint Biometrics, Vol. 2010.
[23].S. Memon, M. Sepasian and W. Balachandran, Review of finger print sensing technologies, *in IEEE International Multitopic Conference, INMIC*, 2008, pp. 226-231.
[24].NeuroTechnology, Bio-i CYTE fingerprint sensor. [Online]. 2010 (08/15), 2010, Available: http://www.neurotechnology.com/fingerprint-scanner-testech-bio-i.html.
[25].T. Harris, Capacitive Scanner, Vol. 2010, pp. 01.
[26]. UPEK, TCS1 TouchChip Fingerprint Sensor, Vol. 2010.
[27].Bergdata Biometrics GmbH, Fingerprint-E field sensors, [Online]. 2010 (03/03), pp. 01. 2010, Available: http://www.authentec.com/
[28].Validity Inc., VFS201 Fingerprint Sensor Product Brief, Vol. 2010, pp. 02, 2010.
[29].J. Han, Z. Tan, K. Sato and M. Shikida, Thermal characterization of micro heater arrays on a polyimide film substrate for fingerprint sensing applications, *J Micromech Microengineering*, Vol. 15, 2005, pp. 282.
[30].G. MSC Vertriebs GmbH, FingerChip™, Atmel‘s Biometric Sensor, Vol. 2010, pp. 01, 2010.
[31].N. Sato, K. Machida, H. Morimura, S. Shigematsu, K. Kudou, M. Yano and H. Kyuragi, MEMS fingerprint sensor immune to various finger surface conditions, *IEEE Transactions on Electron Devices*, Vol. 50, 2003, pp. 1109-1116.
[32].N. Sato, S. Shigematsu, H. Morimura, M. Yano, K. Kudou, T. Kamei and K. Machida. Novel surface structure and its fabrication process for MEMS fingerprint sensor, *IEEE Transactions on Electron Devices*, 52(5), 2005, pp. 1026-1032.
[33].M. Damghanian and B. Y. Majlis, Novel Design and Fabrication of High Sensitivity MEMS Capacitive Sensor Array for Fingerprint Imaging, *Advanced Materials Research*, Vol. 74, 2009, pp. 239-242.
[34].Lapsley, Philip Dean Lee, Jonathan Alexander Pare, Jr., David Ferrin Hoffman, Anti-fraud biometric scanner that accurately detects blood flow, *United States Patent*, 5737439, April 7, 1998.
[35].K. N. Plataniotis, D. Hatzinakos and J. K. M. Lee, ECG biometric recognition without fiducial detection, *in Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research*, 2006, pp. 1-6.
[36].G. Wübbeler, M. Stavridis, D. Kreiseler, R. D. Bousseljot and C. Elster, Verification of humans using the electrocardiogram, *Pattern Recog. Lett.*, Vol. 28, pp. 1172-1175, 2007.
[37].S. Marcel and J. D. R. Millan, Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation, Pattern Analysis and Machine Intelligence, *IEEE Transactions*, Vol. 29, 2007, pp. 743-752.
[38].R. Palaniappan and D. Mandic, EEG Based Biometric Framework for Automatic Identity Verification, *The Journal of VLSI Signal Processing*, Vol. 49, 11/01/, 2007, pp. 243-250.
[39].P. E. Keller, Electronic noses and their applications, in *Proceedings of the IEEE Technical Applications Conference and Workshops (Northcon' 95)*, 1995, pp. 116.
[40].D. Baldisserra, A. Franco, D. Maio and D. Maltoni, Fake Fingerprint Detection by Odor Analysis, *Advances in Biometrics*, pp. 265-272, 2005.
[41].Jim Edmond Riviere, Structure and function of skin, *CRC Press*, 2005, pp. 1-18.
[42].M. Chaberski, Level 3 friction ridge research, *Biometric Technology Today*, Vol. 16, 12, 2008, pp. 9-12.
[43].Anil K. Jain, Yi Chen and Meltem Demirkus, Pores and ridges: High-resolution fingerprint matching using level 3 features, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29, 1, 2007, pp. 15-27.

[44].R. Derakhshani, S. A. C. Schuckers, L. A. Hornak and L. O'Gorman, Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners, *Pattern Recognit*, Vol. 36, 2, 2003, pp. 383-396.
[45].Centre for Unified Biometrics and Sensors. Skin spectroscopy. University of Buffalo, the State University of New York [Online]. 2010 (4/3), pp. 01, Available: http://www.cubs.buffalo.edu/skin.shtml
[46].Ryan R. Emerging biometric technologies. Security infoWatch [Online]. 2010 (03/12), 2009, Available: http://www.securityinfowatch.com/Access+Control/emerging-biometric-technologies
[47].O. Martinsen, S. Clausen, J. B. Nysæther and S. Grimnes, Utilizing Characteristic Electrical Properties of the Epidermal Skin Layers to Detect Fake Fingers in Biometric Fingerprint Systems—A Pilot Study, *IEEE Transactions on Biomedical Engineering*, Vol. 54, pp. 891–894, 2007.
[48].Wei-Yun Yau, Hai-Linh Tran and Eam-Khwang Teoh, Fake finger detection using an electrotactile display system, in *Proceedings of the 10th International Conference on Control, Automation, Robotics and Vision, (ICARCV 2008)*, 2008, pp. 962-966.

---



# Guide for Contributors

## Aims and Scope

*Sensors & Transducers Journal (ISSN 1726-5479)* provides an advanced forum for the science and technology of physical, chemical sensors and biosensors. It publishes state-of-the-art reviews, regular research and application specific papers, short notes, letters to Editor and sensors related books reviews as well as academic, practical and commercial information of interest to its readership. Because of it is a peer reviewed international journal, papers rapidly published in *Sensors & Transducers Journal* will receive a very high publicity. The journal is published monthly as twelve issues per year by International Frequency Sensor Association (IFSA). In additional, some special sponsored and conference issues published annually. *Sensors & Transducers Journal* is indexed and abstracted very quickly by Chemical Abstracts, IndexCopernicus Journals Master List, Open J-Gate, Google Scholar, etc. Since 2011 the journal is covered and indexed (including a Scopus, Embase, Engineering Village and Reaxys) in Elsevier products.

## Topics Covered

Contributions are invited on all aspects of research, development and application of the science and technology of sensors, transducers and sensor instrumentations. Topics include, but are not restricted to:

- Physical, chemical and biosensors;
- Digital, frequency, period, duty-cycle, time interval, PWM, pulse number output sensors and transducers;
- Theory, principles, effects, design, standardization and modeling;
- Smart sensors and systems;
- Sensor instrumentation;
- Virtual instruments;
- Sensors interfaces, buses and networks;
- Signal processing;
- Frequency (period, duty-cycle)-to-digital converters, ADC;
- Technologies and materials;
- Nanosensors;
- Microsystems;
- Applications.

## Submission of papers

Articles should be written in English. Authors are invited to submit by e-mail editor@sensorsportal.com 8-14 pages article (including abstract, illustrations (color or grayscale), photos and references) in both: MS Word (doc) and Acrobat (pdf) formats. Detailed preparation instructions, paper example and template of manuscript are available from the journal's webpage: http://www.sensorsportal.com/HTML/DIGEST/Submition.htm Authors must follow the instructions strictly when submitting their manuscripts.

## Advertising Information

Advertising orders and enquires may be sent to sales@sensorsportal.com Please download also our media kit: http://www.sensorsportal.com/DOWNLOADS/Media_Kit_2012.pdf