TECHNICAL INSIGHTS

SENSOR

TECHNOLOGY ALERT

24th July 2015

1. ELECTRONIC SENSING DEVICE FOR CHEMICAL VAPORS
2. ULTRASONIC FINGERPRINT THREE-DIMENSIONAL SENSOR
3. SMART PIEZOELECTRIC MATERIAL TO HARVEST ENERGY
4. RECENT PATENTS IN THE FIELD OF BIOMETRIC SENSING
5. TECHVISION 2015

1. ELECTRONIC SENSING DEVICE FOR CHEMICAL VAPORS

There are many different types of threats that are faced by airports including terrorist attacks. Terrorist attacks can be through use of guns, explosives, or harmful chemicals. For detecting chemicals at the airport checkpoint, airport operators have traditionally deployed military personnel and sniffer dogs. But these techniques are neither accurate nor reliable. There is hence a need for a device, which can detect and differentiate chemicals and at the same time update the relevant personnel about emergencies or threats.

In chemical and biological threat detection, development efforts are focused on detection technologies that can provide early warning of a threat and analysis results in real time so as to enable field operators to make real-time decisions.

Existing, established technologies for chemical threat detection can have limitations, such as susceptibility to false alarms, limited sensitivity, and inaccuracy due to environmental influences. Faster responses, ability to detect threat agents in lower concentrations are key prevailing needs of the threat detection industry.

Researchers from the Georgia Technology Research Institute have developed a small electronic sensing device to detect chemical vapors present in the atmosphere and alert the user wirelessly. The device will be able to detect harmful gases and explosives. This wireless sensor will also prove valuable to detect and understand air pollution.

The small electronic sensing device is integrated with an array of sensors and radio frequency identification (RFID) and nanotechnology capabilities. The researchers have employed aerosol jet printing to print the circuit on a paper substrate. The device is based on programmable digital technology and because of the digital nature of information or data, it further helps user to easily interpret chemical concentrations. In addition, it will also increase the communication range capability of the device. The device uses 5.8 GHz of radio frequency, and provides additional advantages, such as increased resistance to interference from

materials, such as metals and providing accurate reading about hazardous chemicals and explosives. The researchers were able to detect nitrogen and ammonia gases. In addition, the device is expected to detect food spoilage and telltale chemicals in healthcare. The device is expected to enable several applications in various sectors such as military, environmental, commercial, and healthcare.

The project was self-funded by the Georgia Technology Research Institute. The researchers are currently working on developing pattern recognition software, which will further help to support the functioning of the sensor array. In addition, they are testing the device to identify different chemicals. The researchers are also working on identifying different applications. They are expected to employ a liquid crystal polymer as the printing substrate. Other nanomaterials such as graphene, carbon nanotubes and molybdenum disulfide can also be used in the future to develop the wireless electronic sensing device.

Once the device is successfully commercialized, it is expected to get a good response from the military and defense sector.

Details: Lance Wallace, Director of Communications, Georgia Tech Research Institute, North Ave. NW, Atlanta, GA 30332. Phone: 404-407-7280. E-mail: lance.wallace@gatech.edu. URL: http://www.gtri.gatech.edu

2. ULTRASONIC FINGERPRINT THREE-DIMENSIONAL SENSOR

There are various methods to provide access control such as biometrics (for example, fingerprint sensing or face recognition), access cards, and unique identification number. Among the access control methods, biometrics is gaining traction in different fields due to its low cost of manufacturing and installation. In addition, biometric technology confirms the individual credential of the user unlike the other two methods.

Fingerprint recognition has been a popular form of biometric detection, since it requires minimal effort on the user's part, does not capture information extraneous to recognition purposes, and can have relatively good performance along with a relatively low price.

However, the fingerprint sensor can be easily spoofed. Furthermore, opportunities exist for improving the performance of fingerprint sensors, including reducing noise or distortion in the captured image. There is a need for new or enhanced technology that can provide enhanced security and is also cost effective.

To address the above challenge, researchers from the University of California, Davis, have developed an ultrasonic fingerprint sensor. The ultrasonic fingerprint sensor is capable of acquiring a three-dimensional (3D) image of a person's finger to provide higher accuracy and efficiency. The ultrasonic fingerprint sensor is based on micro-electromechanical systems (MEMS) and ultrasonic imaging technology.

The researchers have developed ultrasonic 3D sensors using two different types of wafers--MEMS and CMOS (complementary metal oxide semiconductor). The MEMS wafer has ultrasound transducers and the CMOS wafer contains signal processing circuitry. These two wafers are joined together and the MEMS wafer is thinned to expose the ultrasound transducer. This process is cost efficient and easy-to-use. The ultrasonic fingerprint image sensor is powered with the help of 1.8V power supply. Once the user places a finger on this chip, the surface of the chip emits an ultrasound pulse. The same transducer also receives echoes returning from the ridges and valleys of the fingerprint's surface. Hence, spoofing is not possible when using these ultrasonic 3D sensors.

The research was supported by the University of California, Berkley and US-based InvenSense Inc. The researchers are currently working on enabling several different applications with the help of ultrasonic 3D sensing technologies. Upon successful commercialization, the ultrasonic 3D sensors have opportunities to gain wide scale adoption by the consumer electronics industry, especially smartphones and tablets OEMs (original equipment manufacturers). The sensors will also have applications in medical diagnostic tools (for personal health monitoring), and multitouch displays. Due to their depth sensing capability, they will also be used for 3D modeling, mobile navigation, airport security, and so on.

Details: David A. Horsley, Professor, Mechanical and Aerospace engineering, University of California, Davis, 1 Shields Ave, Davis, CA 95616. E-mail: dahorsley@ucdavis.edu. Phone: 530-341-3236. URL: http://ucdavis.edu/

3. SMART PIEZOELECTRIC MATERIAL TO HARVEST ENERGY

Rechargeable batteries are commonly used in consumer electronic products such as cell phones, personal digital assistants (PDAs), laptop computers, and wearables. Rechargeable batteries are secondary power sources; that is, primary power sources are used to charge the battery. In most cases, it would be cost prohibitive to manually connect a recharger to each device. One aspect to consider when using rechargeable batteries is that electronics to control the charging profile must often be used. The electronics add to the overall power

dissipation of the device. There is a need for an energy harvesting technique that can use the movements from the human body and convert them into electricity. The technique should be easy to use and cost efficient.

Energy harvesting technology makes use of existing ambient energy sources to power devices. Energy harvesting systems generate electrical energy from various sources, such as solar, vibration, thermal, and human movements. Key types of energy harvesting techniques include photovoltaic, piezoelectric, thermoelectric, magnetic induction, electrostatic, and radio frequency (RF).

Human energy harvesting generates biomechanical or kinetic energy from human motion, which is converted into electrical energy. Energy can also be harvested from biological components such as blood sugar, body heat, and so on. Human power is readily available. Human powered energy harvesting can be used in conjunction with various technologies, such as thermal, kinetic, piezoelectric, and so on. In piezoelectric energy harvesting, piezoelectric effect is used for converting mechanical strain into useable electrical energy.

Researchers from École de technologie supérieure (ÉTS) have developed a chin strap using flexible piezoelectric fiber composites (PFCs). PFC is a smart material, which consists of an integrated electrode and an adhesive polymer matrix. PFC is a smart material, which will function as a sensor, an actuator, and an energy converter. The PFC can harvest energy from the movements of the human jaw.

The basic mechanism behind the chin strap is to measure the movements of the jaw while doing multiple tasks and convert the movements into electricity. The continuous operations of the jaw while eating, chewing, talking can be used to power various low-power electronic devices. According to the researchers, jaw movements while having a meal can harvest around 7 mW of power.

The project was self-funded by the research institute. The device is expected to be deployed in wearable electronic devices. The chin strap also has the potential to be integrated in implantable devices such as hearing aids, cochlear implants, electronic hearing protectors, and communication devices. At present, in experiments with the current prototype and one PFC layer, the device was able to generate 18 microwatts of power. Researchers are currently planning to add more PFC layers to generate more power.

Details: Emmanuelle Berthou, Public Relation, École de technologie supérieure (ÉTS), 1100 Rue Notre-Dame Ouest, Montréal, QC H3C 1K3, Canada. Phone: 514-396-8800. E-mail: emmanuelle.berthou@etsmtl.ca. URL: http://en.etsmtl.ca

4. RECENT PATENTS IN THE FIELD OF BIOMETRIC SENSING

Biometric authentication has become a key method for personal identification. Unique characteristics, such as, fingerprint, face, iris, voice, vein, and palm are used for verifying user identity. The biometric authentication process involves presenting user information for verification purposes and further comparing the presented biometric to a template with the information stored in the database.

Fingerprint recognition is an already established and relatively reliable technology and would likely continue to dominate the biometric authentication market in the coming years. Non-contact biometric access control technologies, such as facial recognition and iris recognition are gathering momentum. Iris recognition with improved scanning range, especially in tandem with face recognition, is finding expanding opportunities.

The biometric sensor market has been experiencing strong demand from the government, financial, retail/consumer electronics, and IT sectors. With the increasing threat of terrorist attacks and the increasing need for efficient identification technologies, biometric identification technologies are evolving, especially in security and surveillance applications. With this security compulsion, governments and law enforcement agencies would be forced to increase spending on biometric technologies and adopt the same. Consumer-based applications, such as, mobile phones and personal data assistants (PDAs) are expected to boost the biometric sensor market in 1 to 2 years.

A recent patent in biometric sensing (US20150193666), which pertains to biometric authentication and spoof detection based on images of the eye is assigned to EyeVerify LLC.

Title	Publication Date/Publication Number	Assignee	Inventor	Abstract
Spoof detection for biometric authentication	09.07.2015; US20150193666	EyeVerify LLC	Reza Derakhshani	This specification describes technologies relating to biometric authentication based on images of the eye. In general, one aspect of the subject matter described in this specification can be embodied in methods that include obtaining images of a subject including a view of an eye. The methods may further include determining a behavioral metric based on detected movement of the eye as the eye appears in a plurality of the images, determining a spatial metric based on a distance from a sensor to a landmark that appears in a plurality of the images each having a different respective focus distance, and determining a reflectance metric based on detected changes in surface glare or specular reflection patterns on a surface of the eye. The methods may further include determining a

				score based on the behavioral, spatial, and reflectance metrics and rejecting or accepting the one or more images based on the score
Continual authorization for secured functions	16.07.2015; US20150199687	Apple Inc.	Byron B. Han	A computing device may determine to execute a secured function. The computing may obtain a biometric of the user of the computing device utilizing one or more biometric sensors associated with the computing device, determine that the biometric matches the biometric of a user authorized to utilize the secured function, and execute the secured function. Whenever during execution of the secured function the computing device determines that the biometric sensor no longer detects the biometric of the user, the computing device may cease execution of the secured function.
Data storage key for secure online transactionS	16.07.2015; US20150199684	Christopher Maus	Christopher Maus	A secure non-volatile solid state memory data key appears similar to a conventional USB flash drive modified to have a physical shape resembling a door key with an eyelet for attaching the data key to a key ring or lanyard. The data key includes a USB port, a microprocessor (effectively serving as the “chip” in the chip-and-pin configuration), and a secure memory for holding secure transaction information, such as credit and debit card numbers, verified personal identification (federated ID), and other secure data. A biometric sensor (e.g., touch sensor or “capcha”) verifies that a person is in physical possession of the data key before permitting access to the secure memory. The touch sensor may be limited to use by a unique individual person through a biometric reader, such as a finger print reader, where the verification finger print is stored on the key rather than the connected host device.
User identification system based on plethysmography	09.07.2015; WO/2015/102588	Apple Inc.	Culbert, Daniel J.	A light emitter and light sensor pair can be used to determine one or more characteristics of a user's vasculature. For example, a pulse oximeter employs a light emitter and a light sensor to measure the percentage of oxygenated blood in a subject. In examples of the present disclosure, light emitters and light sensors can be used to perform biometric identification of a user based on identifying characteristics of the user' s vasculature. For example, light information can be obtained at one or more light sensors, and the information can be compared to stored information associated with a user identity. Based on the comparison, the user of the device can be identified as having the user identity.
Data capable strapband for sleep monitoring, coaching, and avoidance	09.07.2015; WO/2015/103334	ALIPHCOM	Utter, II, Max Everett	ABSTRACT A wireless data capable strapband to detect inflammation, resting heart rate (TRHR), and fatigue may include sensors for generating motion signals in response to body motion (e.g., accelerometry), for generating force signals in response to force exerted by a body portion, for generating biometric signals indicative of biometric activity (e.g., heart rate, respiration, arousal), and for generating location signals

				based on user location. The sensor signals may be processed to monitor parameters that may impact a state of sleep of the user (e.g., time of sleep, quality of sleep, hydration, inflammation, contraction, fatigue, TRHR, accelerometry, arousal of the SNS, etc.). Data from the processed signals may be presented (e.g., visually, sound, email, text message, tactile, webpage, etc.) to the user in a format (e.g., reports notifications, coaching, avoidance) intended to instruct/encourage the user to improve their state of sleep.
Real-time fatigue, personal effectiveness, injury risk device(s)	09.07.2015; WO/2015/103330	ALIPHCOM	UTter, Max Everett	A wireless wearable device to passively detect fatigue in a user may include a suite of sensors including but not limited to accelerometry sensors for generating motion signals in response to a user's body motion, force sensors for generating force signals in response to force exerted by a body portion on the force sensor, and biometric sensors for generating biometric signals indicative of biometric activity including GSR, EMG, bioimpedance, image sensors, and arousal in the SNS. The suit of sensors may operate to passively determine, one or more of TRHR, systemic inflammation (I), contraction (C) (e.g., due to dehydration), stress, fatigue, and mood without any intervention or action on part of the user. The suite of sensors may comprise sensors distributed among a plurality of wireless wearable devices that are wirelessly linked and may share sensor data and data processing in making determinations of fatigue in the user.
Extending user authentication across a trust group of smart devices	02.07.2015; US20150186636	Francis M. Tharappel	Francis M. Tharappel	Particular embodiments described herein provide for a wearable electronic device with a biometric sensor and logic. At least a portion of the logic is implemented in hardware. The logic is configured to receive input data indicative of biometric input and attempt to authenticate the input data based, at least in part, on at least one biometric credential of an authorized user. The logic is configured to establish a wireless connection to a smart device, determine whether the smart device is included in a trust group of one or more smart devices, and send a communication to unlock the smart device when the input data is successfully authenticated and when the trust group includes the smart device.

Exhibit 1 lists some of the patents related to biometric sensing.

Picture Credit: Frost & Sullivan

5. TECHVISION 2015

The TechVision program is the premier offering of Technical Insights, the global technology innovation-, disruption-, and convergence-focused practice of Frost & Sullivan. TechVision embodies a very selective collection of emerging and disruptive technologies that will shape our world in the near future. This body of work is a culmination of thousands of hours of focused effort put in by over 60 global technology analysts based in six continents.

A unique feature of the TechVision program is an annual selection of 50 technologies that are driving visionary innovation and stimulating global growth. The selected technologies are spread across nine Technology Clusters that represent the bulk of R&D and innovation activity today. Each Cluster represents a unique group of game-changing and disruptive technologies that attract huge investments, demonstrate cutting-edge developments, and drive the creation of new products and services through convergence.

Our technology analysts regularly collect deep-dive intelligence on several emerging and disruptive technologies and innovations from around the globe. Interviews are conducted every day with innovators, technology developers, funders, and others who are a part of various technology ecosystems. The respondents are spread across public and private sectors, universities, research institutions, and government R&D agencies. Each technology is rated and compared across several parameters, such as global R&D footprint, year of impact, global IP patenting activity, private and public funding, current and emerging applications, potential adoption rate, market potential, and so on. This organic and continuous research effort spread across several technologies, regions, organizations, applications, and industries is used to generate an annual list of Top 50 technologies that have the maximum potential to spawn innovative products, services, and business models.

Furthermore, we analyse several possible convergence scenarios where two or more of the Top 50 technologies can potentially come together to disrupt, collapse, and transform the status quo. Driven by IP interactivity emanating from each of the top technologies, a whole range of innovative business models, products, and services will be launched at unprecedented speed in the future. We have come up with over 25 such unique convergence scenarios.

The Top 50 technologies we have selected for TechVision 2015 have the power to drive unique convergence and catalyse wide-scale industry disruptions. Frost and Sullivan’s TechVision program empowers you with ideas and strategies to

leverage the innovations and disruptive technologies that can drive the transformational growth of your organization.

Rajiv Kumar

Senior Partner

For more information contact:

techvision@frost.com

Visit us at:

www.frost.com/techvision

Follow us on:

@TechVision_FS

www.frost.com/techvisionlinkedin

Back to TOC

To find out more about TechVision, access http://www.frost.com/techvision Follow us on @TechVision_FS, http://www.frost.com/techvisionlinkedin

To comment on these articles, write to us at tiresearch@frost.com

---

You can call us at: **North America**: +1-843.795.8059, **London**: +44 207 343 8352, **Chennai**: +91-44-42005820, **Singapore**: +65.6890.0275

