Survey of Biometric Authentication and Proposal of New Sensing Mechanism

Hirofumi Miki, Shigeki Tsuchitani

***Abstract*— This paper presented biometric authentication and the advantage of fingerprint-based biometric technology in these applications. After reviewing various types of existing sensing technologies and commercialized fingerprint captures, the problems in previous research and products are summarized. To overcome problems in the previous research and existing technologies, a novel sensing principle was proposed and the fabrication process as well as the results of experimentally demonstrated sensing mechanism was introduced.**

***Index Terms*—Biometric authentication, fingerprint sensor, MEMS, micro heater array.**

I. INTRODUCTION

Along with the rapid popularization of electronic information systems, the need of reliable human identification systems is emergent. To prove someone's identity and prevent identity fraud is extremely important in a variety of situations when one wants to receive a service in social life. For example, for secure access to buildings, networks, confidential databases, and ATMs (Automatic Teller Machine) as well as for the internet transactions. In the absence of robust verification schemes, these systems are vulnerable to the wiles of an impostor. Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict fraud access. However, security can be easily breached in these applications when the password is divulged to an unauthorized user or a badge is stolen by an impostor. The emergence of biometrics has been expected to be promising to address the problems that plague traditional verification methods. Biometrics, described as the science of recognizing an individual based on his/her physiological or behavioral traits, is being to gain acceptance as a legitimate method for determining an individual's identity [1]. Biometric systems have now been deployed in various commercial, civilian and forensic applications as a means of establishing identity.

In immigration authorities, for example an "U.S. VISIT Program" had been started in America at 2004 by DHS (Department of Homeland Security), and picked biometrics information from every immigration [2]. In Japan, the demonstration experiment for the use of biometric authentication had been performed in NRT (Narita International Airport) at 2002 [3], and from Nov. 20th 2007, it has been mandated that all of the foreigners must be extracted their fingerprints and photographing of their faces in the immigration examination [4]. In financial field, Bank of Tokyo-Mitsubishi UFJ, Ltd. (formerly Bank of Tokyo-Mitsubishi, Ltd) adopted biometric authentication systems on ATM for the first time in Japan at Oct. 2004 [3]. According to Nihon Keizai Shimbun (Economic Newspaper of Japan) dated Aug. 26th 2005, the survey results on the security measures of financial facilities that feedback from three metropolitan area (areas around Tokyo, Aichi Prefecture, and Kyo-Han-Shin (Shiga, Kyoto, Osaka and Hyogo Prefecture)), showed that in the point of "security measures" and "image of security measures fullness", Bank of Tokyo-Mitsubishi UFJ got a top reputation outdistancing the runner-up greatly, and many banks including Sumitomo Mitsui Banking Corporation consistently adopted biometric authentication systems too. Recently, biometric authentication systems are growing in usage and popularity even in the area of login from personal computer and cell-phone or smartphone, and there is a growing opinion that biometric authentication is ultimate and safe answer for security. However, different with the traditional methods of password or ID cards, biometrics authentication in fact do not recognize the target by perfect matching but only based on the similarity level with enrolled data, so that there is an inevitable problem of false rejection and false acceptance. Potential imposture authenticating with an artificial biometrics is also a crucial problem. A number of verification systems based on different biometric characteristics have been developed. Among the biometrics like fingerprints, hand geometry, iris, retina, face, hand/finger vein, facial thermogram, signature or voiceprint, biometrics of fingerprints is being held as one of the most secure means today to identify an individual [5]. However, T. Matsumoto reported that gummy fingers, namely artificial fingers that are easily made of cheap and readily available gelatin, were accepted by extremely high rates by 11 particular fingerprint devices with optical or capacitive sensors [6]. Some researchers also reported, in 1998, that four of six fingerprint systems with optical devices accepted silicone fingers [7]. It was known that the fingerprint system in "iphone 5s" easily accepted by the false fingerprint made from residual trace pattern of fingerprint on the iphone screen [8]. To make better use of biometrics authentication, it will be important to well understand the sensing mechanism of verification devices. In order to overcome the problems in existing identification technologies and enable to realize robust automatic authentication systems in social service, we proposed a novel sensing principle for thermal micro fingerprint sensors. In this paper, we will introduce the most widely used biometrics of fingerprint concerning its features and the mostly used fingerprint sensing technologies. We also present our proposed sensing mechanism and results of experimentally demonstrated sensing mechanism.

Hirofumi Miki, Department of Systems Engineering, Wakayama University, Wakayama, Japan, +81(73) 457-8196,
Shigeki. Tsuchitani, Department of Systems Engineering, Wakayama University, Wakayama, Japan, +81(73) 457-8146,

II. Biometric Methods for Personal Identification

Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the persons. They have an edge over the traditional security methods, because they cannot be forgotten, stolen or easily shared or misplaced. Moreover, biometrics-based method requires that the person to be identified be present at the point of authentication to provide his/her biometric measurement. A number of verification systems based on different biometric characteristics have been developed. In these systems, biometrics of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermogram, signature or voiceprint is generally used [9]. However, most of the physical characteristics such as hand geometry, face and voice are very similar for identical twins and automatic verification based on these physical characteristics will fail to distinguish them. By definition, identical twins cannot be distinguished even based on DNA [10].

To realize a robust authentic verification in an automatic system, the used biometric must be:
(i) Universal: everyone possesses the characteristic;
(ii) Collectible: the characteristic is easy to capture;
(iii) Permanent: the characteristic remains invariant over lifetime;
(iv) Distinctive: the characteristic is different for everyone.

Typical biometric-based techniques which being used or being developed for the personal identification are summarized in Table 1. It is claimed that identical twins can be distinguished based on their fingerprint, iris, retina and hand vein patterns [10-12]. In the biometric-based authentication systems, especially, the fingerprint sensor can be made very small size with a low cost that easy to be integrated into a variety of applications including mobile computing and even into a cellular phone. Below the attention was focused on the fingerprint formation to describe its distinguishable characteristics in identical twins.

III. Fingerprint and its Distinctiveness

Fingerprints are fully formed at about 7 months of fetus development. Finger ridge configurations are growing up to adult size but do not change throughout the life except due to accidents such as bruises and cuts on the fingertips. They can also reconstruct the same if not too severe injury [10].

The distinguishing nature of physical characteristics of a person is due to both the inherent individual genetic diversity within the human population and the random processes affecting the development of the embryo [13, 14]. According to Anil K. Jain etc. [10], biological organisms, in general, are the consequence of the interaction of genes and environment. It is assumed that the phenotype is uniquely determined by the interaction of a specific genotype and a specific environment. Physical appearance and fingerprints are, in general, a part of an individual's phenotype. In the case of fingerprints, the genes determine the general characteristics of the pattern. The general characteristics of the fingerprint emerge as the skin on the fingertip begins to differentiate. However, the flow of amniotic fluids around the fetus and its position in the uterus changes during the differentiation process. Thus the cells on the fingertip grow in a microenvironment that is slightly different from hand to hand and finger to finger. The finer details of the fingerprints are determined by this changing microenvironment. A small difference in microenvironment is amplified by the differentiation process of the cells. There are so many variations during the formation of fingerprints that it would be virtually impossible for two fingerprints to be alike. However, since the fingerprints are differentiated from the same genes, they will not be totally random patterns either [15].

Monozygotic twins are a consequence of division of a single fertilized egg into two embryos. Thus, they have exactly identical DNA except for the generally undetectable micro-mutations that begins as soon as the cell starts dividing. Fingerprints of identical twins start their development from the same DNA, so they show considerable generic similarity [16]. However, identical twins are situated in different parts of the womb during development, so each fetus encounters slightly different intrauterine forces from their siblings. Therefore, fingerprints of identical twins have different micro-details, which can be used for identification purposes [17]. Anil K. Jain etc. [10] showed that even though identical twin fingerprints have large class correlation, they can still be distinguished using a minutiae-based automatic fingerprint verification system though with slightly lower accuracy than non-twins. In fact, for more than 100 years, the uniqueness of fingerprint has been acknowledged and exploited in law enforcement [18] and is being held as one of the most secure means today to identify an individual [19]. Because you have more than one finger, multiple fingers could be required, even in specific sequence, to secure the system. You may also have a specific finger to initiate a silent alarm.

IV. Fingerprint-based Authentication Systems

The system is mainly composed of two important parts: *authentication software* and *hardware (fingerprint sensor module)* as shown in Fig. 1.

A. Authentication software

It generally has the following three important components: *Feature extraction module, matching module and decision-making module.*

(1) ***Feature extraction module,*** in which the acquired fingerprint image is processed to extract feature values, for example, the position and orientation of minutiae points in a fingerprint, to create a template.

(2) ***Matching module,*** in which the feature values are compared against those in the template by generating a matching score. For example, in this module, the number of matching minutiae points between the query and the template will be computed and treated as a matching score.

(3) ***Decision-making module,*** in which the user's identity is established or a claimed identity is either accepted or rejected based on the matching score generated in the matching module.

Fingerprint authentication system operates in two modes to recognize fingerprint: *enrollment and authentication.*

Enrollment can be further organized into three steps: *image capture, signature extraction and storage.* With a compact electronic system, all of these phases can be completed in a very short time.

In the enrollment mode, fingerprint data is acquired by the fingerprint sensor and signature (template) is extracted typically with 30 to 40 of minutiae and then stored in a

database. The stored template is labeled with a user identity (e.g., name, identification number, etc.) to facilitate authentication.

Authentication: In the authentication mode, the process follows the same steps as enrollment with the addition of another: *image capture, signature extraction* and then matching.

The only difference with *image capture* during enrollment is that the sensor may not be in the same location or might even be a different type. Due to the maturity of today's software application, with their advanced image filtering and minutiae extraction techniques, different images from different sensors are no longer a significant concern. The template generated by each image with the same software will be compatible. The process of *signature extraction* is the same during authentication as during enrollment because the new signature must be compatible with the reference. Today, there is no compatibility at this level between different software packages, so one must use the same company's software algorithms for both enrollment and recognition [18]. *Matching* consists of comparing the reference signature/template, stored during enrollment and the live template obtained from the user attempting to be recognized. Biometrics distinguishes between two types of matching: 'one to one' which had known as ***Identification*** and 'one to many' which known as ***Verification***. There is quite a significant difference between identification and verification in terms of search and match routines. Identification requires a very efficient matching routine, as a search within millions of fingerprints has to be performed in a short time. Verification only requires a check against one reference, so the computation time is much shorter.

FAR & FRR: Fingerprint recognition, like other biometrics, is not 100% perfect. Standard error rates have been defined. FAR is the *False Acceptance Rate*, the percentage of imposters that may be able to enter the system. FRR is the *False Rejection Rate* or the percentage of true enrollees that are not able to enter the system. The performance of an authentic system can be measured by reporting its FAR and FRR at various thresholds. Both rates must be as low as possible, but are actually antagonists and part of an intricate balancing act. If you make the system harder to enter for an impostor, results to reduce the FAR. You also make the system harder to enter for a true enrollee by raising the FRR. The same occurs in reverse, too.

Matching algorithms Many different algorithm types exist, but direct (optical) correlation is practically not used, because of the lack of efficiency for the large database. Generally, the common shape of the fingerprint is used to pre-process the images, and reduce the search in large databases. Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. Most algorithms are using minutiae. Only the position and direction of these features are stored as the templates for further comparison. Correlation-based techniques require the precise location of a registration point. Some algorithms count the number of ridges between particular points, usually the minutiae, instead of the distances computed from the position.

Very often, algorithms are using a combination of all these techniques. Detailed information about them can be found in references [20] and [21].

Minutiae Discontinuities of fingerprint ridges are called minutiae by which the uniqueness of a fingerprint can be determined combined with the position of the patterns and their relative size. A fingerprint consists of up to 100 ridge endings or minutiae, yet courts in the USA consider that 12 minutiae are sufficient for the legal identification. If at least eight to twelve minutiae are found to be the same, criminal investigation procedures usually consider fingerprints to match [22]. The most basic patterns in fingerprints and the typical minutiae can be found in [22].

Following are minutiae of commonly appearing:

(1) ***Endings:*** the points at which a ridge stops;
(2) ***Bifurcations:*** the point at which one ridge divides into two;
(3) ***Dots****:* very small ridges;
(4) ***Islands:*** ridges slightly longer than dots, occupying middle space between two temporarily divergent ridges;
(5) ***Ponds or lakes:*** empty spaces between two temporarily divergent ridges;
(6) ***Spurs:*** a notch protruding from a ridge;
(7) ***Bridges:*** small ridges joining two longer adjacent ridges;
(8) ***Crossovers:*** two ridges which cross each other;
(9) ***Cores:*** the inner point, normally in the middle of the print, around which swirls, loops, or arches center. It is frequently characterized by a ridge ending and several acutely curved ridges;
(10) ***Deltas:*** the points, normally at the lower left and right hand of the fingerprint, around which a triangular series of ridges center.

Depending on CPU power, typical fingerprint matching solutions can compare thousands of fingerprints and generate probable matches within millisecond. After classification into pattern (typically loop, arch, or whorl), the system notes the positioning of the patterns, and evaluates their relative size.

As easily known, the system performance depends on both the software and the sensor. Bad software or a bad sensor will give bad results and even both a good sensor and software may give bad results if they are not well suited for each other. However, the sensor must be able to capture a good quality image first, otherwise, the software will be unable to extract minutiae and form a representative templates. The image capture device plays a key role in the fingerprint authentication. It is the predominant factor of system price and verification performance for the complete system. Bellow the attention is focused on the previous research of hardware (fingerprint captures) technology.

B. Hardware/fingerprint capture - Previous Research -

A variety-type of fingerprint captures have been proposed and developed. Inking is the traditional ways of fingerprint capture, and still used today. However, this system is expensive, inconvenient and time consuming due to the subsequent digitization. In traditional automatic fingerprint identification system (AFIS), a finger is inked, rolled onto paper, and digitized by a scanner. On the contrary, the live scan fingerprint device can capture a digital fingerprint image in real time [23]. In recent years, we have seen remarkable innovations in these devices, which have reduced the size, lowered the price, and improved the performance.

There are mainly two types of live scan devices: optical and solid-state.

Optical type Optical fingerprint capture is the oldest type and quite common. It is typically based on the frustrated total internal reflection (FTIR) phenomenon [24-26], as illustrated in Fig. 2. Capture devices use a light source and lens to image the fingerprint. The image is captured by a CCD (Charge Coupled Device) or CMOS (Complementary Metal Oxide Semiconductor) camera. When a finger touches the platen, the reflective index is different between the ridge and valley. The light that passes through the glass upon valleys (air on the glass surface) is totally reflected, while that of ridges is not reflected. The reflected light is focused by a lens onto a CCD or CMOS camera where the image is captured. Some variants of less common techniques have been offered by some companies. Kinetic Sciences has proposed a sweeping optical sensor [27]. By means of the sweeping technology, the sensing area can be made smaller. The sweeping action can also clean the device enable to avoid the latent image of the fingerprint. TST (Touchless Sensor Technology AG) removed the prism by directly reading the fingerprint, so the finger does not touch anything, but still need a guide to get the right optical distance [28]. Mitsubishi Electric Corporation introduced a transmission-type touchless sensor in which a near-infrared light source illuminates the upside of a finger, and the fingerprint image is captured at the other side of a finger. A 660-nm light source is used to capture internal ridge-valley patterns under the skin of a finger [29]. Although all these devices use touchless schemes, to the best of our knowledge, there are no reports that the images captured by these devices can be matched and used interoperable with those captured by touch-based sensors [30]. Although there have been many technical improvements in optical-types, this system is still costly and bulky even now. System cost is relatively high because of the cost and mechanical assembly of the prism, lens and camera. Size cannot be reduced substantially due to the required focal lengths, and very often, there is a large distortion of the image because of the difficulty of focusing an image in such a small space. This distortion can be compensated for by software (if one knows the characteristics of the reader), but still, this distortion may even vary from one reader to another of the same model [18].

Solid-state type Although, solid-state sensors (also called silicon or chip sensors) have been proposed in patent literature since the 1980s, it had not been commercially available until the middle 1990s due to the lack of appropriate fabrication techniques. Solid-state sensors were designed to address many of the shortcomings of optical sensors at the time. A distinct advantage of silicon sensor is the ability to integrate additional functions onto the chip. These include A/D (analog to digital converter) conversion or integration of a processor core to perform all fingerprint feature extraction and matching on a single chip. All systems currently available use a matrix of pixels (an array of sensing elements that image the fingerprint via different technologies) and a transducer to convert physical information into electrons. After converted by the transducer, the electronics are relatively simple, and engineers generally use the inexpensive CMOS technologies with their usual advantages and integration capabilities. Usually, resolution is 500 dpi (dots per inch), that is, a pitch of 50 μm (each pixel is a square of 50 μm ×50 μm). This is spelled out in the IAFIS (Integrated Automated Fingerprint Identification System) specification for the U.S. Federal Bureau of Investigation (FBI) [31, 32], and is detailed enough to enable analysis of the ridges and valleys of the fingerprint. Almost all sensors currently have this resolution, but, in commercial systems that is not mandatory. It is debatable what minimum resolution is sufficient for the population of users. Ridges are generally 450 μm wide, so a 225-μm-pitch sensor (112 dpi) is theoretically enough to get the relevant signal information. However, in the real world, fingerprints may be thinner and have narrow ridge spacing for some people and for children, and to allow for a sufficient margin, sensors should be at least 250-dpi (a pitch of 100 μm) [18].

There are mainly three types of solid-state sensors: pressure, capacitance and thermal type.

Pressure-type, as illustrated in Fig. 3, is one of the oldest ideas, because when you put your finger on something, you apply a pressure. Piezoelectric material has existed for years, but unfortunately, the sensitivity is very low. Moreover, when you add a protective coating, the resulting image is blurred because the relief of the fingerprint is smoothed. So, to date, no industrial device has been made.

Capacitance-type, as illustrated in Fig. 4, is currently the most popular technique [33-37]. Capacitors have two electrode plates: one is the metal plate built in the sensor, and the other one is considered to be the skin of the fingerprint. The two electrodes are separated by the passivation layer of the silicon chip and air. This series-connected capacitor *C* is composed of a capacitor between the metal plate and the chip surface and another one between the chip surface and the finger skin. *C* will be at its maximum value when a ridge has contact with the passivation layer. As the distance between the chip surface and the finger skin increases, the capacitance becomes smaller. The ridges and valleys of the fingerprint image can be determined by the measurement of the capacitance differences at each sensor array. A combination of the pressure or tactile sensor structure with the capacitive sensing mechanism has been reported [38, 39], by which the better contrast of pattern images are achieved.

In capacitance-type, the coating must be as thin as possible (a few μm) for the purpose of enough sensitivity. The major problem in this technique is its durability to scratch and tap etc. A significant drawback is its vulnerability to strong external electrical fields, the most dangerous being ESD (Electro-static Discharge). A number of grounding methods are proposed including grounded enclosure, grounded metal ring around the chip, grounded metal “plugs” within the sensor array, and grounded metal mesh as a top chip layer. Another drawback of capacitance-type is its sensitivity to the finger conditions like wet, dry or thinner fingerprint [40].

Thermal-type, Pyroelectric material is able to convert changes in temperature ($\triangle T$) into a specific voltage. This effect is quite large, and is used in infrared cameras. When a fingertip is directly placed on the material as illustrated in Fig. 5, the ridge's temperature is measured, as it is in contact. The valleys do not make contact, so the temperature of the pyroelectric material under the valleys remains almost unchanged. A drawback of this technique is that the image disappears quickly. When one place one’s finger on the sensor, there is a big change of temperature, and therefore signal, but after a short period (less than a tenth of a second), the image vanishes. The finger and the chip have reached thermal equilibrium, and as there is no change in temperature,

there is no signal. This effect disappears when you sweep your finger over the sensor, because of the touch/no touch of ridge/valley [41]. Utilizing this phenomenon, Atmel (formerly Thomson-CSF) developed a thermal sweeping sensor FingerChipTM that enables the detection of the fingerprint patterns and also successfully minimizes device size. However, in this device, the image is weak when the sensor temperature is near the skin temperature, since it measures their temperature differences. This effect disappears when you sweep your finger over the sensor, because of the touch/no touch of ridge/valley [42].The worst case will be happen when the sensor temperature is completely the same as that of the skin.

About sweeping technology: in sweeping technology, the sensing elements are not a single imaging row. Reconstruction is accomplished by determining overlap between adjacent slices being correlated; therefore, there must be some number of rows. This number relates to the speed of sweeping and the reconstruction algorithm requirement on the overlap. The rows of the sensor can be reduced if the sensing speed of the sensor can be increased.

Intermediate type ***Switches,*** extremely tiny silicon switches can be fabricated by MEMS technology. When a finger is pressed onto the sensor surface, the protrusions in the pixels arranged on the sensor surface are pressed down by the ridges of the fingerprint and the switches are closed. This action is converted into electrical signals by the LSI underneath, and is displayed as a single image of the entire fingerprint. The fingerprint image read by the fingerprint sensor can be used for fingerprint identification [43]. But the coating remains a significant problem, and moreover, a binary image is the result, leading to minimal information. No further development has been done with this technique beyond the laboratory.

RF field, this type of sensor is initially similar to a capacitance-type device, although, this sensor in fact injects a low radio frequency (RF) signal into the finger, and each pixel then acts like an antenna. The local electrical field is read, and depending on the local conductivity of the skin, the sensor detects if there is a ridge or a valley. Authentic is proposing this type [41, 44].

Table 2 summarizes fingerprint captures available as a commercial product.

C. Problems in existing fingerprint captures Figures

Variety types of fingerprint sensors have been proposed and some of them have been indeed commercialized already among which the most popular techniques are mainly optical-type and the capacitive-type. However, a number of problems are remaining.

Optical fingerprint device is still costly, bulky and power consumptive, and the image quality is poor due to dirt buildup and image distortion from the focusing misalignment. For the capacitive-type, the problem is its vulnerability to strong external fields, especially to the ESD and parasitic capacitance. Its weakness to the tapping is also one of the difficult problems due to the thin coating for sensitivity. Although the performance is being improved and most of the capacitive sensor makers are declaring that they have solved the ESD problem and show the corresponding value of ESD tolerance, the consistency has been questioned and the durability and mechanical strength are still an issue.

The pyroelectric material based thermal-type developed by Atmel (formerly Thomson-CSF) is relatively a new technique. It can overcome most of the problems in optical and capacitive type fingerprint sensors including the problems of ESD and parasitic capacitance. However, this technology has a problem, namely, the lack of resolution consistency because of its inherent sensing mechanism. When the sensor temperature is near the skin temperature, the detected image becomes weak, and even there is no image at all if the sensor temperature is same to that of the skin.

V. PROPOSAL OF NEW SENSING PRINCIPLE

Because of the inherent features in sensing mechanism, it is difficult to fundamentally overcome the problems in previous sensing technologies. In the lack of the robust and reliable fingerprint capture hardware, automatic authentication systems are vulnerable to the wiles of impostor.

We propose a novel sensing principle to detect fingerprint patterns. The basic concept of the structure and the sensing principle are schematically shown in Fig. 6. The device has a densely arrayed micro heater elements (temperature dependent resistor). To provide thermal isolation, the substrate needs to be a less heat conductive material, and if necessary, thermal insulation layer or cavity should be arranged under the heater elements to reduce the heat transfer to the substrate. When a fingertip is pressed on the sensor surface, the heater elements which in contact with the ridge of the fingerprints, for example E1, will show less of temperature rise than that of facing to the fingerprint valley, for example E2, because of the different thermal path between the two situations. The ridge acts as a heat sink, while the valley acts as a thermal insulator due to the presence of air. When a pulse voltage is applied to each heater element, element E1 will show a lower of temperature-rise than element E2 as schematically shown in Fig. 6-b. The temperature-rise differences between E1 and E2 will be appeared as the electrical resistance change differences. The value of different resistance can be easily converted into electrical signals by circuits, and can be used as the information of user's fingerprint patterns.

The proposed fingerprint capture has the following advantages over the established technologies. Since it measures the temperature differences corresponding to touching ridges versus non-touching valley, there is no need of optical components and no need of worry about the effects of ESD. Different to the pyroelectric-based technology, heat is transferring from the sensor elements to the fingertip during capture, so the signal will not vanish naturally, and the detected image will not be affected by the ambient temperature. Consistent and reliable robust sensing can be obtained. Furthermore, there are not special obstacles in the fabrication of this type of the sensors having the features of a low cost and small size. Employing a pulsed input, less of power consumption is promised due to the possibility of extremely small thermal capacity of the sensing elements.

VI. RESEARCH APPROACH

In this work, we performed two approaches of research to realize the proposed fingerprint capture, i.e. silicon-based approach and polyimide film based approach. In the *silicon-based approach*, the aim was, firstly, to take the advantages of silicon inherent merits of possible integration

with IC on the same sensor chip, and its well-established micro machining technology. Secondly, to clear up the design points in the applicable structure of arrayed thermal sensors. In the *polyimide film based approach*, the aim was to better use of its inherent characteristic of very low thermal isolation (three-order magnitude higher than silicon), and well balanced comprehensive material properties including mechanical, electrical and chemical. In addition, its properties of micromachining and flexibility could enable this approach to a wider range of technical and application extensions.

In the silicon-based approach, the material is silicon in both the substrate and the sensing element for the simple of fabrication process. Using silicon as the sensing element there is another advantages in addition to the process design. For example, by doping the right concentration of some impurity, the electrical resistivity and TCR (temperature coefficient of resistance) of the sensing element can be well-controlled [45-48], useful for thermal sensor design.

In the polyimide film based approach, the substrate is 50μm-thick Kapton polyimide film and the sensing element is sputtered thin platinum film micro resistors. Platinum shows a very high chemical stability with a reasonably high value of TCR (0.00392/K) [49]. Its resistance is particularly linear with temperature and can be used in a quite wide range of temperature (10~1000 K). In this paper, the results of polyimide film based approach will be presented mainly.

VII. Device Fabrication and Sensing Principle Demonstration

A. Structures and materials

In thermal sensor, the most sensitive parameter for the structure and material selection is substrate and its thermal conductivity. PI film possesses extremely low thermal conductivity (λ: 0.12 W $m^{-1}K^{-1}$ for Kapton PI film), which is three orders lower than that of silicon material (λ: 150 W $m^{-1}K^{-1}$). PI film also possesses a unique combination of properties and can retain its excellent properties of thermal and electrical insulation, mechanical strength, chemical resistance, dimensional stability and the attractive characteristics of flexibility under a wide range of operating conditions [50, 51]. PI film can also be micromachined by wet etching or laser technique. Due to its unique material properties, by using the PI film as the thermal sensor substrate an improved thermal isolation and better sensitivity are promising. Furthermore, because, there is no need of thermal isolation cavity, better of the mechanical strength can be obtained with simple structure. Generally, a large number of sensing elements are involved with a small pitch in the 2-D array sensing systems. By utilizing 3-D interconnection technology, the problem of complicate overlapped wiring in the 2-D array sensing systems can be avoided.

Sensing elements of thin metal film can be directly deposited on the PI film substrate by vacuum deposition or sputtering. Copper, nickel and platinum film can be used as the sensing elements. They have positive TCR with approximately linear temperature dependence. At room temperature, the coefficient $(1/R)$ (dR/dT) ranges 3.9×10^{-3} ~ 6.5×10^{-3} K^{-1}. Both the copper and platinum have a TCR of near 4×10^{-3} K^{-1} [52].

Copper: copper resistance offers the most linear temperature dependence with TCR of 4.260×10^{-3} K^{-1} for temperatures from 0 to 100℃. Copper resistances, however, have two disadvantages that strongly limit their use:

(i) At 0℃ the resistivity of copper is less than one sixth of that of platinum with about the same TCR; when the geometrical sizes of copper and platinum are same to each other, the sensitivity of a copper resistance exhibits only one sixth of platinum;
(ii) Copper begins to oxidize above 100℃, and deteriorates rapidly above 180℃.

Nickel: nickel has a high temperature coefficient of 6.81×10^{-3} K^{-1}. Its resistivity, however, is lower than that of platinum and the non-linearity of its resistance versus temperature characteristic is higher.

Platinum: platinum has a reasonably high temperature coefficient of 3.92×10^{-3} K^{-1} and its resistance is particularly linear with temperature [53]. Platinum resistor has a nearly constant TCR, i.e. an output that is directly proportional to temperature over a significant temperature range. More importantly, it has a high chemical stability, which enables platinum to be used as a temperature reference standard. The best stability is achieved in platinum, when the resistances made from above metals are used in air or in a mixture of helium and a small amount of oxygen [54]. Compared to other metals, platinum is relatively expensive, but, by MEMS technology the amount of platinum that is required for the sensing element is very small amount with sub-micron thickness which can make platinum a cost comparable to other materials. From Table 3, where platinum is compared to other materials, it can be concluded that, for a given resistance value, platinum always offers the possibility of smaller volume and smaller thermal mass sensors. This property has been enhanced considerably with the adoption of thin- film sensors that utilize a minimum amount of platinum.

When using platinum film as the sensing element and depositing to the PI film, the problem is its poor adhesion to the PI film surface. A bridge or an adhesion tie layer is required. Chromium, titanium, nickel, tantalum and palladium are often used as the tie layers. We used a 20nm-thick titanium layer as the adhesion promoter. In our process, we performed PI film surface pretreatment firstly by light wet etching in a strong alkaline solution TPE3000 (supplied by Toray Engineering Co., Ltd., Japan) before sputtering titanium layer. TPE3000 is composed of 20wt% KOH solution and 20~40wt% aliphatic amine compound C_2H_7NO. It can hydrolyze PI and polyester compounds.

B. Fabrication process

The ridges of human fingerprint are generally 450 μm wide, so, a 225-μm-pitch sensor (112 dpi) is theoretically enough in order to get the relevant signal information [55]. We fabricated 200-μm pitch of sensor element array as the first generation prototype of the PI film-based approach, which is enough pitch for the experiment to demonstrate the proposed sensing principle. It is not a problem to fabricate a prototype, which have finer pitch of element array (<100 μm), by means of the presented process technology. The limitation of through-hole size by wet etching can be overcome employing

laser technology, with which as small as 5-μm-diameter of uniform through holes can be created on the PI film substrate.

Figure 7 shows the schematic drawing of the fabrication process: (A) is top views, and (B) is cross-sectional views. The starting material is 50-μm thick Kapton PI film. In Fig. 7-(a), by PI film wet etching technology, Φ60-μm of through holes is created. Then, PI film chemical pretreatment is performed in a strong alkaline solution TPE3000 at the condition of 70℃/7sec, in order to promote adhesion of thin metal film to the PI film. In (b) & (c), by photolithography and electroless copper-plating technology, the through hole interconnection is realized between the upper side heater pad and backside electrical feed-through. A 1-μm thick heater pad and electrical feed-through as well as the through hole wiring are created by electroless plating technology at the same process. In (d), by photolithography, platinum sputtering and lift-off patterning, one- dimensionally arrayed heater elements are created on the upper side surface of PI film substrate. 20nm thick titanium film is sputtered firstly as the adhesion tie layer, followed by 200nm thick platinum layer which acts as the sensing elements. Radio frequency (RF) magnetron sputtering equipment RSC-3ERD is used in our fabrication process. The whole fabrication process is simple, cost effective and realized at a low temperature range (<130℃) on the non-silicon and flexible substrate. The fabricated sensor wafer is flexible enough to be attached to non-planar curved surface as show in Fig. 8 shows the schematic drawing of the fabricated prototype structure. The proposed sensor structure and the fabrication technology will be useful for a variety of extended applications of 2- or 3-D distribution sensors with high resolution, and high sensitivity. The low- temperature process will enable the device in a state of higher reliability.

C. Main characteristics of the prototype

TCR of the sensing elements: TCR was obtained by measuring the sensing element's resistance variation in the precisely controlled resistive oven by slowly changing its temperature. The temperature was checked from the display of the oven, and confirmed by measuring with a thermocouple thermometer at the same time. The detection circuit is shown in Fig. 9. A constant direct current I_S was used to drive the circuit. The DC power I_S drives a precise measuring current through the conducting lead wire L1 and L4. The conducting lead wire L2 and L3 measure the voltage drop across the heater element R_h. If the temperature coefficient α is independent of temperature, the relationship between the resistance and the temperature (*R*-*T*) of the material can be written as

$$R(T) = R(T_0)(1+\alpha(T-T_0)) \qquad (1)$$

Where, T_0 is the ambient temperature. The TCR value of the heater element (Pt/Ti film) derived from the experimental result was $2.9\times10^{-3}\ K^{-1}$.

Thermal response: The thermal response of the heater element, which driven by a square-wave pulse voltage, was measured. The heater element's temperature can be calculated from the TCR value and the measured resistance variations of the heater. Very fast temperature response was realized on the heater element due to its excellent thermal isolation from the substrate, and the small thermal capacity of the heater element. Experimental results show that, in about 0.1 μs of time, the heater element's temperature was risen from the room temperature of 24℃ to the near 300℃. The maximum temperature of the heater can also be adjusted by the input power according to the situation of applications. Short of response time is a great advantage in the densely arrayed (e.g. hundreds of 2-D array) high-resolution applications, enable to realize the whole response in *ms* order of time by the small power consumption.

Demonstration of sensing principle: The fabricated prototype as shown in Fig. 8 was used in experiment. The electrical resistance of the heater element was 150Ω at the room temperature. A 4- wire type detecting circuit was used and driven by 25.5mA of direct constant current. By scanning the fingerprint model on the sensor surface, the temperature (or resistance) change on the heater element could be measured. From the temperature change versus scanned step, the stripe patterns were detected. When the micro- heater element is in contact with the ridges of the fingerprint model, its temperature reaches to 122℃, while when it is facing to the valleys of the fingerprint model, the temperature became 134℃. Between the ridge and valley, 12℃ of the temperature differences are generated on the heater element. From the detected temperature differences on the heater elements, the micro patterns of the finger print model are clearly detected. By means of the circuit technology and denser array of micro heater elements, this sensor device could be used for the application of micro fingerprint sensors. The skin consists of three main layers [56] – epidermis (20μm), dermis (200μm) and subcutis (2000μm). Each layer has its specific structure and functions. Epidermis layer is seen on the surface of the skin. It is made up of cells called keratinocytes, which are stacked on top of each other, forming different sub-layers. The dermis consists mostly of connective tissue and is much thicker than the epidermis. It is responsible for the skin's pliability and mechanical resistance and is also involved in the regulation of the body temperature. The subcutaneous layer below the dermis consists of loose connective tissue and much fat. It acts as a protective cushion and helps to insulate the body by monitoring heat gain and heat loss. Because of the complicate skin layer structure, it is not as easy as photocopy of fingerprint patterns to fabricate artificial fingertip having fingerprint patterns. From the complicate layer structure and its mechanical and thermal characteristic as well as the fingerprint patterns of the fingertip, the proposed thermal type fingerprint capture will be useful to overcome the problems in the previous work.

VIII. CONCLUSION

Through the bibliographic survey, it was clear that there is a lack of reliable verification schemes in the increasingly popular field of electronic information systems. Many existing technologies and commercially available fingerprint captures may possess inherent problems in these applications. The author presented a novel sensing principle of micro heater array fingerprint sensor, described the fabrication process and demonstrated the proposed sensing mechanism by experiments. The proposed idea and the researched results could be useful for the goal to overcome problems in the existing techniques and products, as well as for the establishment of reliable automatic authentication systems.

REFERENCES

[1] Arun Ross and Anil K. Jain, Multimodal Biometrics: An overview, *Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria)*, pp. 1221-1224, September 2004.

[2] NSTC, "BIOMETRICS in Government POST-9/11 Advancing Science and Enhancing Operations", August 2008, http://itlaw.wikia.com/wiki/Biometrics_in_Government_Post-9/11:_Advancing_Science,_Enhancing_Operations

[3] IPA (information-technology promotion agency, Japan), Security Center, "Installation of Biometric Authentication Systems and Collection of Operation Cases", November, 2009. http://www.ipa.go.jp/security/fy20/reports/bio_sec/documents/bio_case_20.pdf

[4] Special issue, "Breakthrough in Biometric Authentication", http://itpro.nikkeibp.co.jp/article/COLUMN/20060130/228114/?rt=nocnt

[5] A. K. Jain, A. Ross, and S. prabhakar, "An introduction to biometric recognition", *IEEE Trans. On Circuits and Systems for Video Technology*, Vol. 14, pp. 4-20, Jan 2004

[6] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino, Impact of Artificial "Gummy" Fingers on Fingerprint Systems, Proceedings of the conference Optical Security and Counterfeit Deterrence Techniques IV, Part of IS&T/SPIE's Electronic Imaging 2002,Proc. SPIE Vol. 4677, pp275-289, (http://cryptome.org/gummy.htm) .

[7] David Willis, Mike Lee, Six biometric devices point the finger at security, Journal of Network Computing, 9(10), 84-96 (1998).

[8] http://www.gizmodo.jp/2013/09/iphone_5s_37.html

[9] Arun Ross, Anil Jain, Information fusion in biometrics, Pattern Recognition Letters 24 (2003) 2115-2125.

[10] Anil K. Jain, Salil Prabhakar, Sharath Pankanti, On the similarity of identical twin fingerprints, Pattern Recognition, 35 (2003) 2653-2663.

[11] Takeshi Hajika, Approach of iris identification technique by Oki Electric Industry, Mechatronics, June (2002) 96-99.

[12] I.D.Technica, A Novel individual identification system using vein patterns, Safety and Management, Jan (2000) 49.

[13] R.G. Steen, DNA and Destiny: Nature and nurture in human behavior, Plenum press, New York, 1996.

[14] N.L. Sagal, Entwined Lives: Twins and what they tell us about human behavior, Plume, New York, 2000.

[15] E.P. Richards, Phenotype vs. Genotype: Why identical twins have different fingerprints? http://www.forensic-evidence.com/site/ID_Twins.html

[16] W. Bodmer, R. McKie, The Book of Man: The quest to discover our genetic heritage, Viking, 1994.

[17] H. Cummins, C. Midlo,R. Fingerprints, Palms and Soles: An introduction to dermatoglyphics, Dover Publications Inc., New York, 1961.

[18] Jean-Francois Mainguet, Marc Pegulu and John B. Harris, Fingerprint recognition based on silicon chips, Future Generation Computer Systems 16 (2000) 403-415.

[19] Janathan Roberts, Silicon fingerprint sensors, Biometric Technology Today, Vol. 8, Issue 5, 1 May 2000, pp.8-10.

[20] Biometrics, http://perso.wanadoo.fr/fingerchip/biometrics/types/fingerprint.htm

[21] Biometric education, http://www.barcode.ro/tutorials/biometrics/fingerprint.html

[22] http://www.tst-ag.com/touch/fing-ID.html.

[23] Xiongwu Xia, Lawrence O'Gorman, Innovations in fingerprint capture devices, Pattern Recognition 36 (2003) 361-369.

[24] M. Kawagoe, A, Tojo, Fingerprint pattern classification, Pattern Recognition, 17 (3) (1984) 295-303.

[25] I. Fujieda, Y. Ono, S. Sugama, Fingerprint image input device having an image sensor with openings, US Patent 5446290, 1995.

[26] R.D. Bahuguna, T. Corboline, Prism fingerprint sensor that uses a holographic element, Appl. Opt. 35 (26) (1996) 5242-5245.

[27]http://biometrics.mainguet.org/types/fingerprint/fingerprint_sensors_productsi.htm

[28] System for the touchless recognition of hand and finger lines US 6404904 B1, http://www.google.com/patents/US6404904

[29] E.Sano, T.Maeda, T. Nakamura, M. Shikai, K. Sakata, M. Matsushita, and K. Sasakawa, Fingerprint authentication device based on optical characteristics inside a finger, Proc. Of Computer Vision and pattern Recognition Workshop, pp. 27-32 (2006).

[30] Donghyun Noh, Heeseung Choi, Jaihie Kim, Touchless sensor capturing five fingerprint images by one rotating camera, Optical Engineering , 50(11) 113202 (November 2011).

[31] IAFIS Image quality specification CJIS-RS-0010 (V4) Appendix F & G, August 24, 1995.

[32] P.T. Higgins, Standards for the electronic submission of fingerprint cards to the FBI, J. Forensic Identification 45 (4) (1995) 409-418.

[33] Jeong-Woo Lee, Dong-Jin Min, Jiyoun Kim, and Wonchan Kim, A 600-dip Capacitive Fingerprint Sensor Chip and Image-Synthesis Technique, IEEE Journal of Solid-State Circuits, Vol. 34, No. 4, April 1999, pp. 469-475.

[34] Stefan Jung, Christofer Hierold, Thomas Scheiter, Paul Werner von Basse, Roland Thewes, Karl Goser, and Werner Weber, Intelligent CMOS Fingerprint Sensors, Proceedings of the Transducers'99, The 10th International Conference on Solid-State Sensors and Actuators, Sendai, Japan, June 7-10, 1999, pp. 966-969.

[35] Hiroki Morimura, Satoshi Shigematsu, and Katsuyuki 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, pp. 724-731.

[36] C. Tsikos, Capacitive fingerprint sensor, US Patent 4353056, 1982.

[37] D.R. Setalk, Electric field fingerprint sensor apparatus and related methods, US Patent 5963679, 1999.

[38] P.REY, P. CHARVET, M.T. DELAYE, S. ABOU HASSAN, LETI-CEA/Grenoble, A High Density Capacitive Pressure Sensor Array For Fingerprint Sensor Application, Proceedings of the Transducers'97, Chicago, USA, 1997, pp. 1453-1456.

[39] Richard J. De Souza and Kensall D. Wise, A Very High Density Bulk Micromachined Capacitive Tactile Imager, Proceedings of the Transducers'97, Chicago, USA, 1997, pp. 1473-1476.

[40] Ken Horizoe, Fingerprint identification technology and security, Mechatronics, 2002.4, pp. 102-105.

[41] Fingerprint sensing techniques, http://perso.wanadoo.fr/fingerchip/biometrics/types/fingerprint_sensors.htm

[42] ATMEL, http://biometrics.mainguet.org/types/fingerprint/fingerprint_sensors_productsi.htm#Atmel

[43] Pressure MEMS Fingerprint sensor, http://biometrics.mainguet.org/types/fingerprint/fingerprint_sensors_physics.htm#tactile

[44] Authentec [http://www.authentec.com]

[45] Toyota Central R&D Labs., Inc., "Piezoelectric semiconductors and its applications", 1970.

[46] W. R. Runyan, "Silicon semiconductor technology", McGraw-Hill, New York, 1965.

[47] Helmut F. Wolf, "Silicon Semiconductor Data", Pergamon Press, New York, 1969.

[48] G. Bertolini, A. Coche, "Semiconductor Technology", North-Holland, Amsterdam, 1968.

[49] J. W. Gardner, "Microsensors, Principles and Applications", John Wiley & Sons, Chichester, 1994.

[50] http://www.kapton.dupont.com/

[51] Catalogue, Kapton Polyimide film, DU PONT-TORAY CO., LTD., Japan.

[52] T. Ricolfi, J. Scholz, "Sensors, A comprehensive survey, Volume 4, Thermal Sensors", VCH, 1990.

[53] J. W. Gardner, "Microsensors, Principles and Applications", John Wiley & Sons, Chichester, 1994.

[54] G. C. M. Meier and A. W. van Herwaarden, "Thermal sensors", Institute of Physics Publishing Bristol and Philadelphia, 1994.

[55] Jean-Francois Mainguet, Marc pegulu and John B. Harris, Fingerprint recognition based on silicon chips, Future Generation Computer Systems 16 (2000) 403-415.

[56] Skin structure, http://skincare.dermis.net/content/e01aufbau/e660/e661/index_eng.html

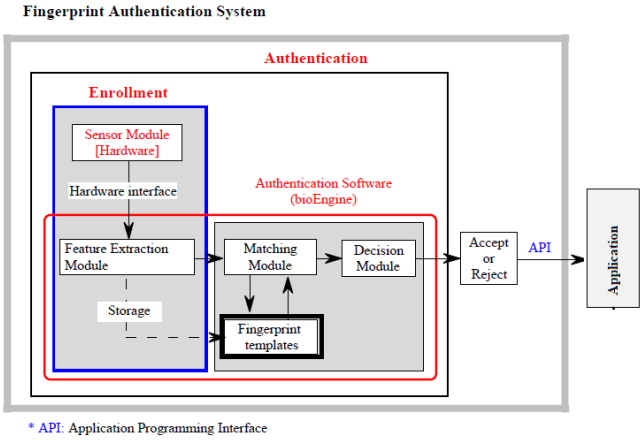


Fig. 1. Fingerprint-based authentication system

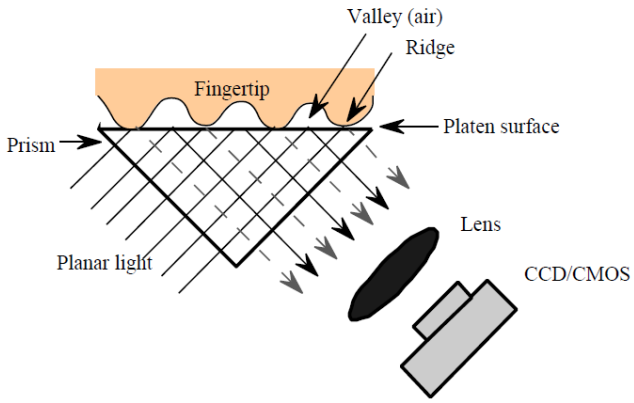


Fig. 2. Sensing principle of optical-type fingerprint sensor.

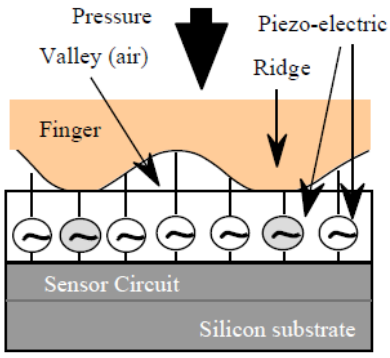


Fig. 3. Sensing principle of pressure-type fingerprint sensor.

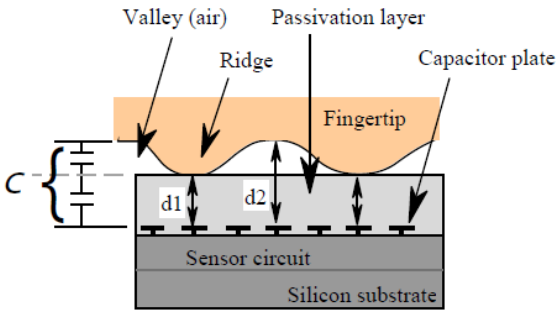


Fig. 4. Sensing principle of capacitance-type fingerprint sensor.

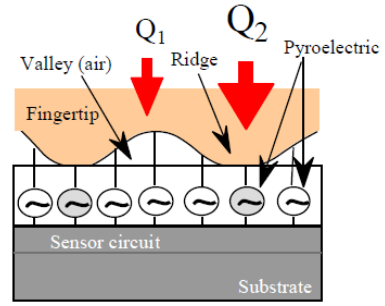
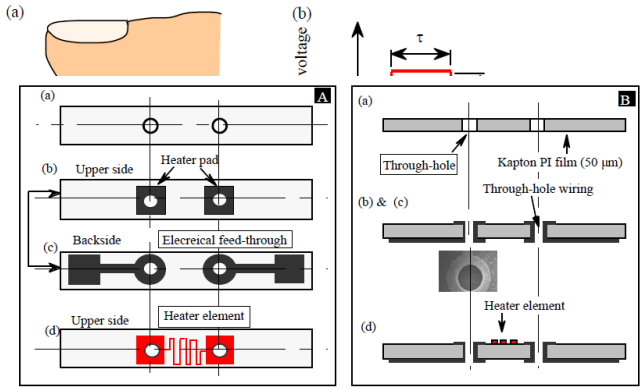


Fig. 5. Sensing principle of pyroelectric-based thermal fingerprint sensor.



n **Fig. 7.** Fabrication process of micro heater array having interconnected through hole metal film wiring: (A) top views, and (B) cross sectional views.

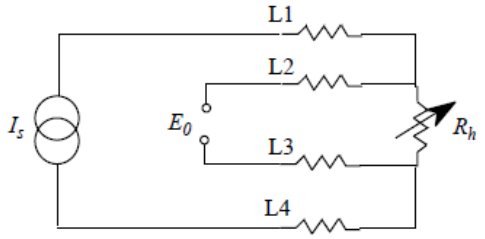


Fig. 9. Detection circuit for measuring TCR of the heater elements.

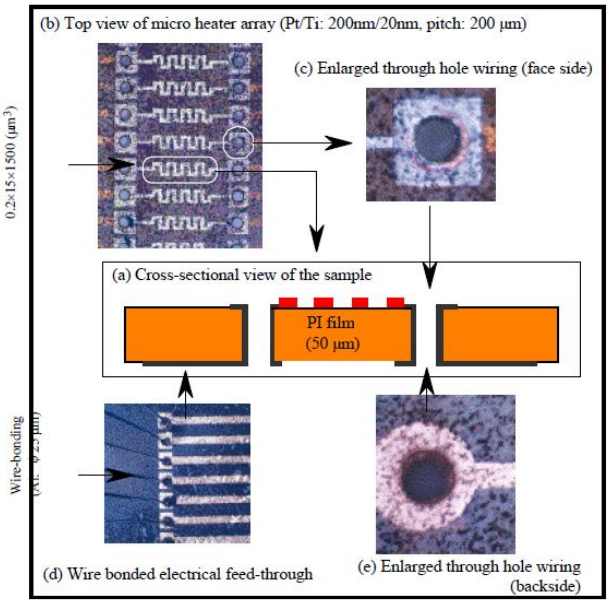


Fig. 8. Fabricated prototype structure: (a) cross-sectional view of the sample; (b) top view of the one-dimensionally arrayed micro heater elements; (c) top view of the enlarged through hole wiring; (d) bottom view of the feed-through with wire bond; (e) bottom view of the enlarged through hole wiring.

Table 1. Typical biometric methods for personal identification

Biometrics	Information capturing	Identical twins Distinguishable	Advantages	Drawbacks
Fingerprint	Pattern or minutiae by fingerprint capture (Optical, capacitive, thermal...)	Yes	Reliable & permanent Size, cost Consumption Convenience	Psychological rejection
Iris	Iris patterns by CCD camera	Yes	Reliable & permanent Contactless Less of compulsary	Downsize, cost Consumption Psychological burden
Retina	Blood vessel patterns on retina by near-infraed-rays scan combine with CCD sensor	Yes	Same as above	Same as above
Hand vein	Vein patterns by near-infraed-rays scan combine with CCD sensor	Yes	Reliable& permanent	Downsize, cost Consumption
Face	Layout and contrasting by CCD camera	No	Contactless Verification from a distance	Downsize, cost Consumption Imposter
Voiceprint	Voiceprint by microphone	No	Convenient Low cost	Imposter
Signature	Online input with pen	No	Same as above	Imposter
Hand geometry	Geometry by CCD camera	No	Simple technique	Downsize, cost Consumption Imposter

Table 2. Comparison of different fingerprint sensors [19, 23, 41-44]

Company (Sensor name)	Sensor type	Resolution (dpi)	Image size (pixels)	Image capture area (in/mm)	ESD tolerance	Interface	Others
Digital Persona, Inc. (U.are.U 4000)	optical	512	290 x 364	0.57 x 0.71 14.6 x18.1	> 15 kV	USB	Size: 79 x 49 x 19 mm (3.11 x 1.93 x 0.75 in) Operating: 5~35°C.
SecuGen (FDU02)	optical	500	260 x 300	0.5 x 0.6 13 x15	> 15 kV	USB	Size: 62 x 21 x 32 mm (2.4 x 0.8 x 1.3 in) Operating: 0~40°C.
Kinetic Sciences Inc. (KC-901)	optical linear array	257~901		0.75 x N 19 x N	NA	USB	Swipe-type, large capture area
NEC_ SecureFinger (SA301-10/11)	optical	800	567 x 472	0.71 x 0.6 18 x15	NA	RS-232C	Size: 50x42 x11.5 mm (1.97x1.65 x0.45 in) Operating: 0~40°C.
Identix (DFR-200)	Optical	380	254 x 254	0.67 x 0.67 17 x 17	8 kV	USB	Size: 96x60x31 mm (3.78x2.36x1.2 in) Operating: 0~55°C
Fujitsu (MBF310)	CMOS capacitive	500	218 x 8	0.43 x 0.02 10.9 x 0.4	8kV	8bit MCU	Size: 16.1x6.5x1.2mm (0.63x0.26x0.05 in) Swipe-type. sweep rate: 20cm/sec (8in/sec) Operating: -20~+85°C.
Veridicom (FPS200)	CMOS capacitive	500	256 x 300	0.5 x 0.6 12.8 x15	> 8 kV	USB, MCU SPI	Sensitivity is adjusted by changing the discharge current and discharge time.
UPEK (from ST Micro) (TouchChip TCS1CD)	CMOS capacitive	508	256 x 360	0.71 x 0.5 18 x 12.8	±15 kV	8bit RAM	Size : 27x20.4x3.5 mm (1.06 x 0.8 x 0.14 in) Operating: 0~40°C.
Sony (FIU-600-N03)	CMOS capacitive	317	128 x192	0.4 x 0.6 10.2 x 15.4	NA	USB	Size : 69x52x25 mm (2.72 x 2.05 x 0.98 in) Pttern matching. Operating: 5~35°C.
Atmel (FingerChip™) formerly Thomson-CSF	Pyroelectric (thermal array)	500	8 x 280	0.02 x 0.55 0.4 x 14	±9 kV	USB	Requires temperature differential between fingertip and sensor. Critical at 33±5°C. Swipe type. Operating: 0~70°C.

Table 3. Properties of copper, nickel and platinum material [13]

Properties \ Materials	Cu	Ni	Pt
Resistivity (20°C, μΩ cm)	1.673	6.84	10.6
Density (20°C, g cm^{-3})	8.92	8.9	21.45
Length (a) (cm)	1173	287	185
Mass (mg)	205	50.1	77.9
Heat capacity (b) (mJ K^{-1})	79	22	11
TCR ($10^{-3}K^{-1}$)	4.3	6.81	3.92

(a) a wire of 0.05 mm having a resistance of 100 Ω at 20°C.
(b) values at 25°C.