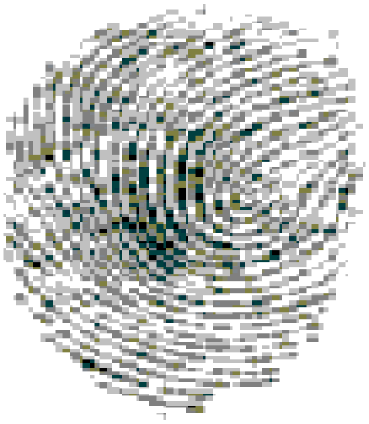
FINGERPRINT AUTHENTICATION



By

T.Karthik

IT (3 / 4),

	MAIL	PHONE
Karthik-	karthiktangirala@live.in	9912892397

ASTRACT :-

Biometrics, the science of applying unique physical or behavioral characteristics to verify an individual's identity, is the basis for a variety of rapidly expanding applications for both data security and access control. Numerous biometrics approaches currently exist, including voice recognition, retina scanning, facial recognition and others, but fingerprint recognition is increasingly being acknowledged as the most practical technology for low cost, convenient, and reliable security. Fidelica Microsystems' new and exclusive technology overcomes the limitations of previous systems and sets a new standard for compact, reliable and low-cost fingerprint authentication.

THE BASIS OF FINGERPRINT AUTHENTICATION

Although fingerprints have been used as a means of identification since the middle of the 19th century, modern fingerprint authentication technology has little in common with the ink-and-roll procedure that most people associate with fingerprinting. In order to appreciate the distinction and understand modern fingerprint authentication technology, one needs to understand the basis of a fingerprint.

A fingerprint is composed of ridges, the elevated lines of flesh that make up the various patterns of the print, separated by valleys. Ridges form a variety of patterns that include loops, whorls and arches as illustrated in Fig. 1. Minutiae are discontinuities in ridges, and can take the form of ridge endings, bifurcations (forks), crossovers (intersections) and many others.

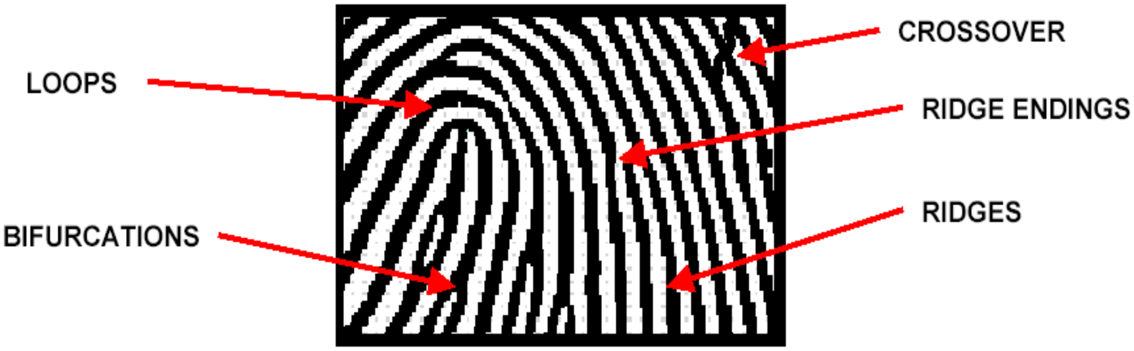


Fig. 1.

Fingerprint authentication is based on a subset of features selected from the overall fingerprint. Data from the overall fingerprint is reduced (using an algorithm application that is usually unique to each vendor) to extract a dataset based on spatial relationships. For example, the data might be processed to select a certain type of minutiae or a particular series of ridges. The result is a data file that only contains the subset of data points . the full fingerprint is not stored, and cannot be reproduced from the data file. This is in contrast with ink-and-roll fingerprinting (or its modern optical equivalent), which is based on the entire fingerprint.

Modern forensic fingerprinting, with files on the order of 250kB per finger, is used in large scale, one-to-many searches with huge databases, and can require hours for verification. Fingerprint authentication, using files of less than 1000 bytes, is used for one-to-one verification and give results in a few seconds.

HOW FINGERPRINT AUTHENTICATION WORKS

In use, fingerprint authentication is very simple. First, a user enrolls in the system by providing a fingerprint sample. The sensor captures the fingerprint image. The sensor image is interpreted and the representative features extracted to a data file by algorithms either on a host computer or a local processor (in applications such as cellular handsets). This data file then serves as the users individual identification template. During the verification process, the sequence is repeated, generating an extracted feature data file. A pattern matching algorithm application compares the extracted feature data file to the identification template for that user, and the match is either verified or denied. State-ofthe-art processor, algorithm and sensor systems can perform these steps in a second or two.

MODERN FINGERPRINT AUTHENTICATION TECHNOLOGY

Fingerprint authentication can be based on optical, capacitance or ultrasound sensors. Optical technology is the oldest and most widely used, and is a demonstrated and proven technology, but has some important limitations. Optical sensors are bulky and costly, and can be subject to error due to contamination and environmental effects. Capacitance sensors, which employ silicon technology, were introduced in the late 1990’s. These offer some important advantages compared to optical sensors and are being increasingly applied. Ultrasound, utilizing acoustic waves, is still in its infancy and has not yet been widely used for authentication.

I ----- SILICON-BASED SENSOR TECHNOLOGY

Silicon-based sensors have a two-dimensional array of cells, as shown in Fig. 2. The size and spacing of the cell is designed such that each cell is a small fraction of the ridge spacing. Cell size and spacing are generally 50 microns, yielding a resolution of up to 500 dpi, the FBI's image standard. When a finger is placed on the sensor, activating the transistors that underlay each individual cell captures the image. Each cell individually records a measurement from the point on the finger directly above the cell as shown in Fig. 3.

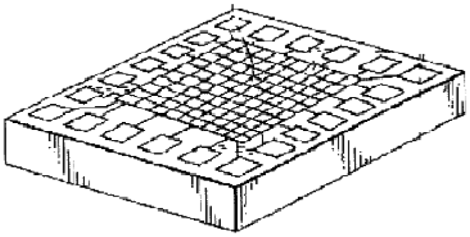


Fig. 2.

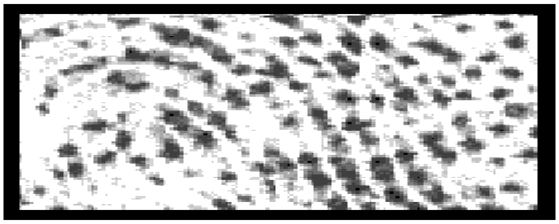


Fig. 4.

Though different vendors use different physical properties to make the measurement, the data is recorded as the distance, or spacing, between the sensor surface and that part of the finger directly above it. However, distance measurement has some inherent weaknesses, which are overcome by Fidelica Microsystems' novel technology, as described below.

FIG 3

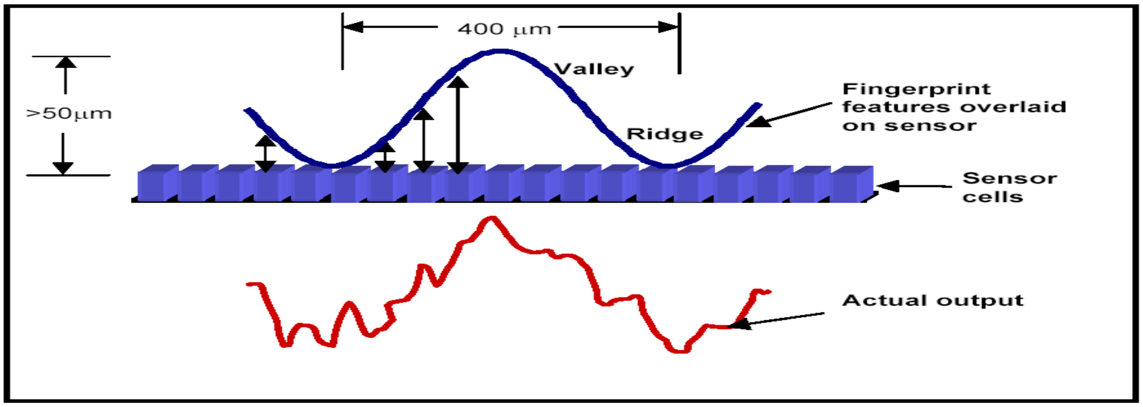


Fig. 3.

The set of data from all cells in the sensor is integrated to form a raw, gray-scale fingerprint image as shown in Fig. 4. Fingerprint imaging using a continuum of distance measurements results in an 8-bit gray scale image, with each bit corresponding to a specific cell in the two-dimensional array of sensors. The extreme black and white sections of the image correspond to low and high points on the fingerprint. Only the high points on the fingerprint are of interest, since they correspond to the ridges on the fingerprint that are used to uniquely identify individuals. Therefore, the **8-bit gray-scale image** must be converted into a binary, or **bitonal, image** using an additional procedure in the feature extraction algorithm. This process is a common source of error, since there could be many false high points or low points due to dirt, grease, etc., each of which could result in a false minutia extraction, and hence, introduce additional error in the matching process.

The feature extraction algorithm is then used extract the specific features from the fingerprint that make up the individual's unique data file. This data file serves as the user's individual identification template, which is stored on the appropriate device. During verification, the imaging and feature extraction process is repeated, and the resulting data file compared with the users identification template by pattern matching software to verify or deny the match.

II ------ FIDELICA MICROSYSTEMS' TECHNOLOGY

PRESSURE SENSING SCIENCE

Fidelica Microsystems' sensor technology is unique among commercially available fingerprint authentication systems. Fidelica Microsystems uses a thin film-based sensor array that measures pressure to differentiate ridges from valleys on a fingerprint. This is in contrast to distance measurement, which is the basis of all other commercially available sensors, whether optical or capacitance (silicon-based).

The sensor is architecturally and physically similar to the silicon-based sensors in terms of cell size and spacing, and therefore offers similar resolution. However, when a finger in placed over the sensor, only the ridges come in contact with the individual pressure sensing cells in the two-dimensional array, whereas no other part of the finger contacts the sensor. As a result, only those cells that experience the pressure from the ridges undergo a property change. To record the image, the array is scanned using proprietary electronic circuits. With an appropriate threshold setting, a distinction can be made between those cells that experience pressure and those that do not.

The Fidelica Microsystems sensor employs a resistive network at each cell location. Each cell incorporates a structure similar to those employed in the micro-electromechanical system (MEMS) industry. Upon the application of a fingerprint, the structures under the ridges of the fingerprint experience a deflection, and a change in resistance results. This change in resistance is an indication of the presence of a ridge above the cell being addressed. In principle, although the resistance value is an analog value, the difference between the resistance in the pressed and unpressed states is large enough that, with an appropriate threshold setting, one can easily distinguish between the presence or absence of a ridge with high resolution and accuracy.

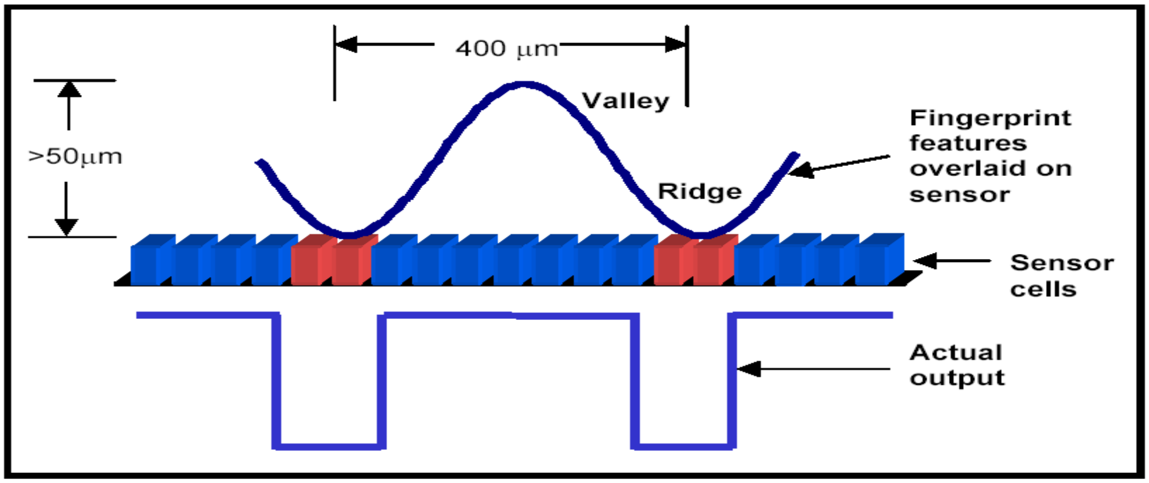
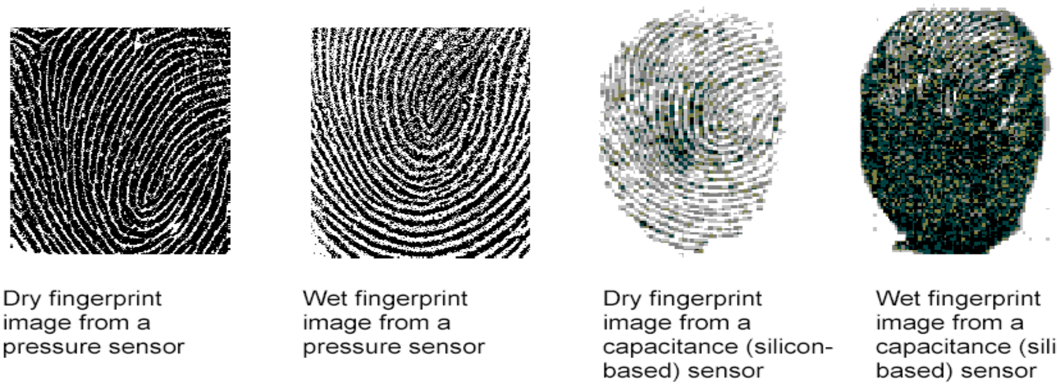


Fig. 5.

Pressure measurement offers some inherently powerful performance advantages over the measurement of spacing. The first is improved accuracy of ridge and valley detection. Because the sensor detects pressure rather than distance, it readily differentiates between ridges and valleys. A valley exerts no pressure at all on the cell underneath it (as shown in Fig. 5, whereas all the cells underneath a ridge would record a pressure. With the appropriate threshold setting, this results in a “digital” response: the cell either records a ridge or a valley. In contrast, the spacing measurement technique used by competing methods generates a continuum of measurements or a gray scale, which must be corrected for noise reduction, gray scale adjustment, gain and sensitivity adjustment.

As a result of using pressure rather spacing to image the fingerprint, the Fidelica Microsystems sensor is considerably less sensitive to interference from dirt and grease on the finger or the sensor, wet or dry fingers, and other effects. In the presence of moisture, sweat, grease or other oils, which are usually present as thin layers on the surface of the skin, there is usually no effect on a pressure-based sensor, whereas with a distance-based measurement, these thin layers cause significant distortion in the resulting image output. An example of a fingerprint image under wet and dry conditions for a Fidelica Microsystems sensor versus a competitive sensor is shown in Fig. 6.



Dry fingerprint image from a pressure sensor

Wet fingerprint image from a pressure sensor

Dry fingerprint image from a capacitance (silicon-based) sensor

Wet fingerprint image from a capacitance (silicon-based) sensor

Fig. 6.

AUTHENTICATION ALGORITHMS

As described above, a fingerprint sensor, unto itself, has limited utility for a customer. Only the combination of a sensor with an authentication algorithm adds value. Fidelica Microsystems' strategy is to be algorithm agnostic. Algorithms can be loosely divided into two broad classes, correlation-based and minutiae-based. Correlation-based authentication algorithms use longer-length–scale information in the fingerprint image (the fingerprint ridges). These algorithms are preferred for convenience applications. Minutiae-based authentication algorithms use shorter-length-scale information Minutiae-basedauthentication algorithms are preferred for high security applications.

In order to fulfill all customer needs, Fidelica Microsystems has developed its own minutiae-based algorithm, which, to the best of our knowledge, has performance that is as good if not better than any other algorithm currently available. Fig. 7 shows a raw fingerprint image captured with Fidelica Microsystems' sensor and the same image after processing using our algorithm with the minutiae locations highlighted.

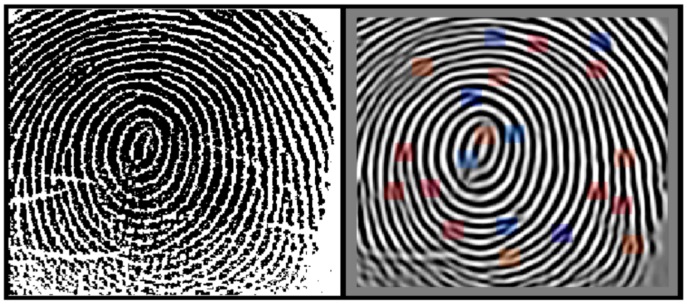


Fig. 7

SUMMARY

Fidelica Microsystems' sensor solves the size, cost and reliability problems that have limited the widespread application of fingerprint authentication. These are the most important criteria to any authentication system, and Fidelica Microsystems directly addresses each:

• Size: Fidelica Microsystems' sensor chip is small . about the size of a postage stamp . and can be integrated into practically any device . cell phone, keyboard, mouse and door lock, nearly any security application imaginable.

• Cost: Fidelica Microsystems' sensor chip is thin-film-based, rather than silicon-based, and can be manufactured on plastic, glass and many other substrates. Thin-film manufacturing is substantially less expensive than other methods. Fidelica Microsystems' sensor chips can be produced and distributed for less than $5 in quantity.

• Reliability and Sensitivity: Fidelica Microsystems' thin-film technology, combined with unique control circuitry, yields a more durable and reliable sensor.

References :

1.Google Search..---- Finger Print Authentication.

2. Fidelica Microsystems,their particular site.