Fingerprint-Sensoren

Biometrie-Sensoren werten Körpereigenschaften von Personen aus und führen somit zur zweifelsfreien Authentisierung. Der Daumen oder ein anderer beliebiger Finger als Schlüssel ist nicht kopierbar und kann auch nicht verloren gehen oder weiter gegeben werden.

Allgemeines

Biometrische Systeme werten Körpereigenschaften und Verhaltensweisen zur Identifizierung von Personen aus. Jeder Mensch trägt ständig seine individuellen Körpermerkmale mit sich herum und kann diese nicht verlieren, weitergeben oder jemandem leihweise überlassen. Es liegt also im Grunde genommen nichts näher, als diese Merkmale für eine eindeutige Identifizierung und zur Erteilung von Zutrittsberechtigungen zu nutzen.

Wichtig ist bei einem biometrischen Identifikationsverfahren, dass die Erfassung mit einem vertretbaren Aufwand möglich ist, das Verfahren einfach in der Handhabung ist und eine hohe Akzeptanz bei den Anwendern findet.

Zu den eindeutigsten Identifikationsmerkmalen eines Menschen gehört der Fingerabdruck, da bisher keine identischen Fingerabdrücke von unterschiedlichen Personen bekannt sind. Andere biometrische Merkmale zur Identifizierung bzw. Authentisierung von Menschen sind Stimmmuster, die Netzhaut oder die Iris der Augen, die Gesichtsgeometrie und die Handgeometrie.

Die Erfassung und die Auswertung von Fingerabdrücken ist in der Kriminaltechnik seit vielen Jahrzehnten bekannt und hat zur eindeutigen Überführung von vielen Straftätern geführt. Während früher die Fingerabdruck-Auswertung ausschließlich von Hand durchgeführt wurde, bieten heute moderne Sensorsysteme automatische Erfassungs- und Auswertemöglichkeiten.

Während viele biometrische Körpermerkmale des Menschen einzigartig sind, stehen zur Erfassung des Fingerabdrucks ausgereifte Identifikationstechniken zur Verfügung. Werden mehrere Finger zur Identifikation vom System erfasst, so funktioniert das Ganze auch noch, wenn ein Finger „einmal ein Pflaster tragen muss".

Der zu überprüfende Finger muss, je nach Sensorart, nur noch kurz auf den Sensor aufgelegt oder über diesen gezogen werden. Die Aufnahme dieses biometrischen Körpermerkmals kann also sehr schnell und schmerzlos erfolgen.

Andere biometrische Erfassungssysteme, wie z. B. die Stimmenanalyse, könnten bereits bei einer Erkältung vollständig versagen. Die Fingerabdruck-Erkennung ist daher das am meisten verbreitete Verfahren, da auch unter rauhen Alltagsbedingungen eine reibungslose Funktion relativ einfach möglich ist.

Auch wenn die Bedienung des Erfassungssystems denkbar einfach ist, wird von den Benutzern jedoch ein Mindestmaß an Kooperation erwartet. Denn je nach eingesetztem Sensor muss der Finger wenige Sekunden flach aufgelegt werden oder es ist erforderlich, diesen langsam über den Sensor zu ziehen. Nur wenn der Sensor auch wirklich die Möglichkeit hat, die einzelnen Fingerlinien zu erfassen, erfolgt keine Ablehnung.

Fingerprint-Sensor als Ersatz für Pin-Code

Der Zugriff auf viele technische Systeme erfolgt heute über sogenannte PIN (Personal Identification Number) -Codes. Angefangen beim Handy, über Computer, Laptops, Internet und Netzwerkzugriffe, bis hin zur Geldkarte werden zur Freischaltung Pin-Codes benötigt. Da diese PINs meistens 4-stellig sind, besteht nur eine Wahrscheinlichkeit von 1:10000, dass diese auf Anhieb richtig erraten werden. Bei drei zulässigen Versuchen besteht aber nur noch eine Sicherheit von 1:3000.

Die größte Gefahr besteht jedoch nicht darin, dass die PIN-Nummer zufällig erraten wird, sondern im sorglosen Umgang mit diesen Geheimnummern. Kaum jemand ist in der Lage, sich mehrere PINs unverwechselbar zu merken, da es sich in der Regel nicht um selbstgewählte Nummern handelt. Also werden Geheimzahlen notiert und nicht selten fahrlässig verwahrt. So kleben Internet- und Netzwerkzugangsnummern auf Haftzetteln am Monitor oder die Geheimzahl der Eurocheque-Karte wird zusammen mit dieser aufbewahrt.

PIN-Nummern lassen nicht erkennen,

Bild 1: Fingerprint-Zugangssystem mit USB-Port

wer sie tatsächlich benutzt und im Falle eines Missbrauchs kann der Anwender den sorgfältigen Umgang mit seiner Geheimzahl kaum beweisen.

Die Vorteile eines Fingerprint-Sensors liegen nun auf der Hand. Niemand muss sich Geheimnummern merken, es kann keine unbeabsichtigte oder beabsichtigte Weitergabe erfolgen und man hat die Zutrittsberechtigung jederzeit in Form der eigenen Finger dabei.

Fingerprint-Sensor zur Zeiterfassung

Die in den meisten Firmen eingesetzten Zeiterfassungs-Systeme arbeiten mit Magnetkarten oder Passiv-Transpondern. In der Regel werden mit den Magnetkarten oder Transpondern die einzelnen Arbeitszeit- und Pausenbuchungen vorgenommen und in vielen Fällen erfolgt damit auch die Zutrittskontrolle.

Auch wenn diese Systeme sehr zuverlässig und sicher funktionieren, besteht immer die Gefahr, dass Mitarbeiter die Magnetkarten bzw. Transponder vergessen oder verlieren. Des Weiteren ist leicht ein Missbrauch möglich, indem ein Mitarbeiter den Code-Träger jemand anderem überlässt. Fingerprint-Sensoren bieten hier den Vorteil, dass absolut kein Missbrauch möglich ist und niemand den Code-Träger vergessen oder verlieren kann. Entscheidendes Argument ist, dass zur Freigabe einfach außer den eigenen Fingern nichts benötigt wird und man sich auch nichts merken muss.

Fingerprint-Sensoren in Verbindung mit PCs

In Verbindung mit PCs ist der Einsatz von Fingerprint-Sensoren am einfachsten, da an Hardware nur der eigentliche Sensor mit minimaler Peripherie benötigt wird. Die komplette Auswertung der vom Sensor erfassten Daten kann im PC erfolgen.

Bei einigen Notebook-Herstellern, wie z. B. Acer, sind bereits Fingerprint-Sensoren integriert. Ohne Freigabe durch den Fingerabdruck eines autorisierten Benutzers wird das Notebook unbrauchbar. Im Gegensatz zu Passwörtern ist die Gefahr des Missbrauchs so gut wie ausgeschlossen. Für die Nutzung des Notebooks können natürlich auch mehrere verschiedene Nutzer eingerichtet werden. Die Daten werden verschlüsselt auf der Festplatte abgelegt, sodass bei einem Ausbau des Laufwerks die Daten nicht mit einem anderen Rechner gelesen werden können.

Für die Nachrüstung bei bestehenden PCs gibt es Fingerprint-Zugangssysteme mit USB-Port (Abbildung 1). Das externe Fingerprint-Identifikationssystem wird einfach an einen USB-Port des PCs angeschlossen, die auf der CD mitgelieferte Software installiert und bis zu 3 Finger von Berechtigten registriert.

Das Login über das Windows-Betriebssystem ist nur mit dem richtigen Fingerabdruck möglich.

Das Erkennungsprogramm wird in das Windows-Screensaver-Passwortsystem eingebunden, sodass der Screensaver erst nach Verifikation des Fingerabdrucks beendet wird.

Andere Hersteller, wie z. B. Siemens, bieten PC-Mäuse mit integriertem Fingerprint-Sensor an. Auch hierbei erfolgt dann der Anschluss über den USB-Port des Rechners.

Interessante Möglichkeiten für die Zukunft

Für zukünftige Anwendungen gibt es viele interessante Möglichkeiten. So kann mit diesen modernen Sensoren die Authentisierung an Geldautomaten, der Zugriff auf Internet-Anschlüsse und Netzwerke, das Scharfschalten von Alarmanlagen usw. geregelt werden.

Eingebaut in Handys steht eine komfortable Alternative zum PIN-Code zur Verfügung und wenn die Integration des Sensors mit der kompletten Auswerte-Elektronik in Chip-Karten möglich wird, kann ausschließlich der Karteninhaber diese nutzen.

Sehr interessante Anwendungen sind auch im Automotive-Bereich zu finden. Beispielsweise kann dann in modernen Kraftfahrzeugen der Zündschlüssel entfallen. Durch den Einbau eines Fingerprint-Sensors sind nur noch autorisierte Personen, dessen Fingerabdrücke zuvor gespeichert werden, in der Lage, das Fahrzeug zu starten.

Da das Fahrzeug dann automatisch die am Lenkrad sitzende Person „erkennt", können sämtliche individuellen fahrerabhängigen Einstellungen, wie die Sitzposition, die Einstellung der Spiegel, die Lenkradposition usw., vom Fahrzeug selbstständig nach der Identifikation vorgenommen werden. Ja, selbst der Lieblings-Radiosender ist auf Wunsch automatisch vorwählbar.

Biometrische Sensoren sind des Weiteren hervorragend für den Einsatz in Alarmanlagen und in elektronischen Schließsystemen geeignet. Um die kaum noch überschaubare Flut von Passwörtern und PIN-Nummern einzudämmen, werden in Zukunft mehr und mehr biometrische Erfassungssysteme zum Einsatz kommen. Dann werden auch die Preise für die derzeit noch recht teuren Sensoren sich weiter nach unten bewegen.

Aufbau von Fingerprint-Sensorsystemen

Zum Aufbau eines Fingerprint-Sensorsystems gehört neben dem Sensor eine leistungsfähige Hard- und Software zur Auswertung der vom Sensor erfassten Hautstrukturen. Mit einem einfachen Mikrocontroller können die komplexen Algorithmen nicht mehr verarbeitet werden.

Mit dem Sensor werden die Papillarlinien der Haut an den Fingerkuppen aufgezeichnet. Die Verarbeitung der Informationen muss dann ein leistungsfähiger DSP (Digitaler Signalprozessor) oder bei PC-Anwendungen der PC selber übernehmen.

Weitere Miniaturisierung, sowohl des Sensors als auch der verarbeitenden Systeme, werden in Zukunft neue Anwendungsgebiete erschließen.

Während der Einsatz in Handys sicherlich nicht mehr sehr lange auf sich warten lässt, ist der Fingerprint-Sensor in der Smart-Card noch eine interessante Zukunftsvision.

Neben der möglichst kleinen Baugröße erfordern mobile Systeme zusätzlich einen geringen Stromverbrauch.

Fingerabdruck-Sensoren liefern in der Regel ein Graustufenbild, das mehrere Kilobyte groß ist. Mit Hilfe der Software müssen dann die charakteristischen Merkmale extrahiert werden. Als charakteristische Merkmale gelten z. B. Start- und Endpunkte von Kurvenverläufen.

Die als Referenz abgespeicherte Datenmenge reduziert sich dann, je nach System, auf ca. 50 bis wenige 100 Byte. Aus den abgespeicherten Merkmalen kann das Original jedoch nicht wieder rekonstruiert werden.

Viele namhafte Halbleiter-Hersteller befassen sich mit der Entwicklung von Fingerprint-Sensoren oder sind bereits mit Systemen am Markt vertreten. Bekannte Sensoren arbeiten auf optischer, kapazitiver oder Temperaturbasis. Andere Senso-

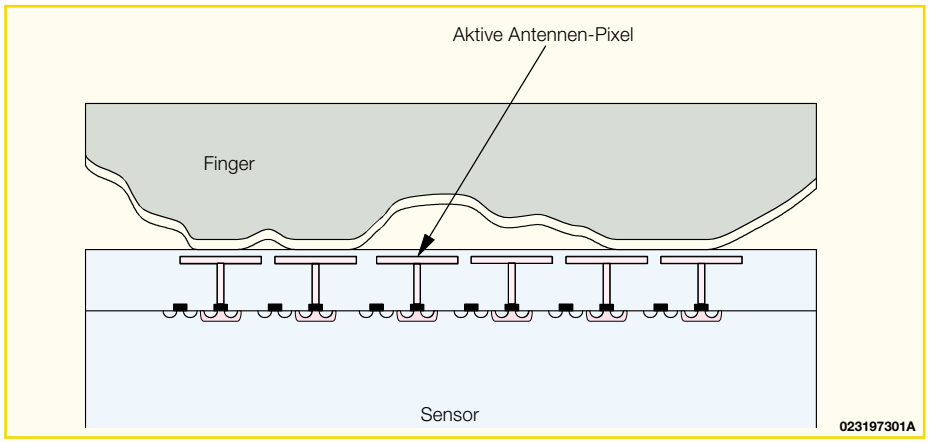

Bild 2: Der FingerTip-Sensor von Infineon misst die Kapazität zwischen den einzelnen Fingerlinien und der Sensoroberfläche

ren wiederum ermitteln das elektrische Feld zwischen den Papillarlinien der Haut an den Fingerkuppen.

Eine wesentliche Rolle für die Kosten spielt dabei die Sensorfläche. Daher setzen einige Hersteller auf Zeilensensoren, über die der zu erfassende Finger dann langsam zu ziehen ist. Unabhängig von der Sensor-Technologie wird zuerst ein Abbild des Fingers aufgezeichnet. Daraus werden die charakteristischen Merkmale extrahiert und mit den Referenzmerkmalen berechtigter Personen verglichen.

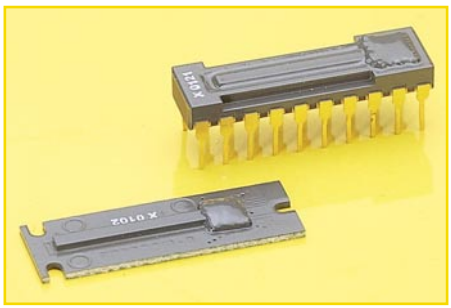

Bild 3: Die Atmel-Zeilensensoren

Zu unterschiedlichen Zeiten aufgezeichnete Fingerabdrücke werden nie vollkommen identisch sein, da die Position des zu erfassenden Fingers von Mal zu Mal abweicht. Verschmutzungen und kleine Verletzungen führen ebenfalls zu unterschiedlichen Daten.

Die Software darf also keine Abweisung vornehmen, wenn eine zuvor eingestellte Anzahl von Übereinstimmungen erreicht ist. Wie genau die Aufnahme des Fingers mit dem Referenzabdruck übereinstimmen muss, ist in der Regel über die Software konfigurierbar. Bei sehr hoher Sicherheit kommt es dann zeitweise zur Abweisung von berechtigten Personen und wenn das System als sehr bequem konfiguriert ist, kann es gelegentlich zur Akzeptanz von nicht berechtigten Personen kommen. Eine exakte Übereinstimmung der biometrischen Daten kann nicht erreicht werden, da niemals genau dieselben Bedingungen herrschen.

Wichtige Parameter zur Beurteilung der Fehlerraten sind die False Acception Rate (FAR), die False Rejection Rate (FRR) und die Equal Error Rate (EER).

Die False Acception Rate beschreibt den prozentualen Anteil fälschlich zugelassener Personen, die False Rejection Rate den Anteil berechtigter Personen, die abgewiesen wurden und bei der Equal Error Rate sind FAR und FRR gleich groß.

Je nach Anwendung kann ein 1:1-Vergleich oder ein 1:n-Vergleich erforderlich sein. Ein 1:1-Vergleich ist grundsätzlich einfacher, da der zu überprüfende Fingerabdruck nur mit einem einzigen Referenzabdruck verglichen wird. Beim 1:n-Vergleich muss der erfasste Fingerabdruck mit allen gespeicherten Fingerabdrücken einer Datenbank verglichen werden. Dies erfordert natürlich leistungsfähigere Prüfverfahren und, je nach Größe der Datenbank, eine erheblich höhere Rechengeschwindigkeit.

Anhand von einigen Beispielen wollen wir nun die Funktionsweise von verschiedenen Sensorkonzepten betrachten.

Infineon-Sensor-„FingerTip"

Infinion nutzt zur Aufnahme des Fingerabdrucks eine Messung der Kapazität zwischen dem Halbleiter und der Hautoberfläche. Die Oberfläche, des in CMOS-Technologie hergestellten Sensors, besteht aus einem Array von 280 x 224 Sensorelektroden und erlaubt eine Auflösung von 513 dpi (Dots per Inch).

Abbildung 2 verdeutlicht die prinzipielle Funktionsweise dieses Sensors. Der Abstand der Haut zu den einzelnen Sensorelektroden ist abhängig von den Papillarlinien. Das mit über 60000 Sensorelektroden erzeugte Rohbild ist ein Ausschnitt des Fingerabdrucks. Die gesamte Sensorfläche beträgt ca. 100 mm^2. Aus dem Rohbild werden dann die charakteristischen Merkmale extrahiert und mit den abgespeicherten Informationen verglichen.

Zur Erzeugung des Rohbildes ist natürlich mehr als die reinen Sensorelemente erforderlich. Diese Komponenten sind jedoch direkt auf dem Chip integriert, sodass vom Fingerprint-Sensor die Daten in Form von 8 Bit pro Pixel geliefert werden. Zur Auswertung der vom Sensor gelieferten Rohdaten ist dann noch eine leistungsfähige Hardware und natürlich die Software zum Extrahieren der charakteristischen Merkmale erforderlich.

Die Abmessungen des Infineon-Sensors betragen 18 mm x 21 mm bei nur 1,5 mm Dicke. Der Anschluss erfolgt über einen flexiblen Leiterplattenverbinder.

Atmel-FingerChip

Bei der elektronischen Erfassung von Fingerabdrücken setzt Atmel auf einen Zeilensensor, der mit wesentlich weniger Chipfläche auskommt und bei entsprechenden Stückzahlen kostengünstiger herzustellen ist. Abbildung 3 zeigt diesen Sensor in den beiden zur Verfügung stehenden Gehäusevarianten (20-Pin-Keramik-DIP oder Chip-on-Board). Die eigentliche Sensorfläche beträgt nur 0,4 x 14 mm.

Bei diesem Konzept wird der zu erfassende Finger nicht aufgelegt, sondern muss langsam über die Sensoroberfläche gezo-

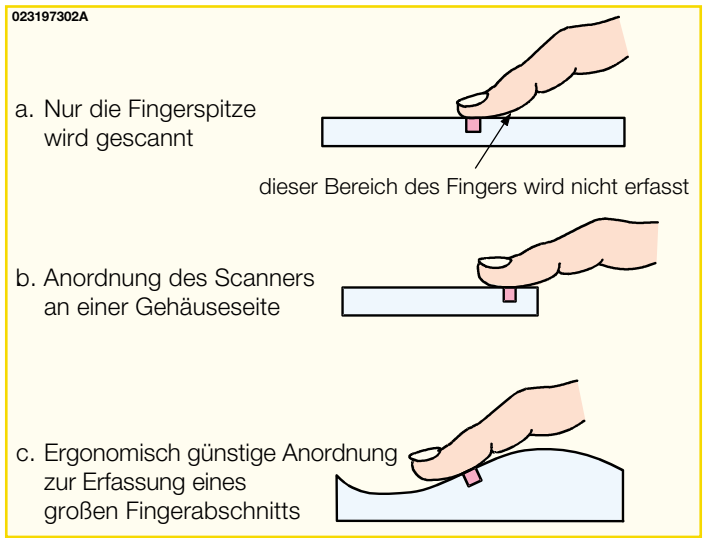

Bild 4: Die mechanische Anordnung des Sensors im Gehäuse hat einen wesentlichen Einfluss darauf, welcher Bereich des Fingers gescannt wird.

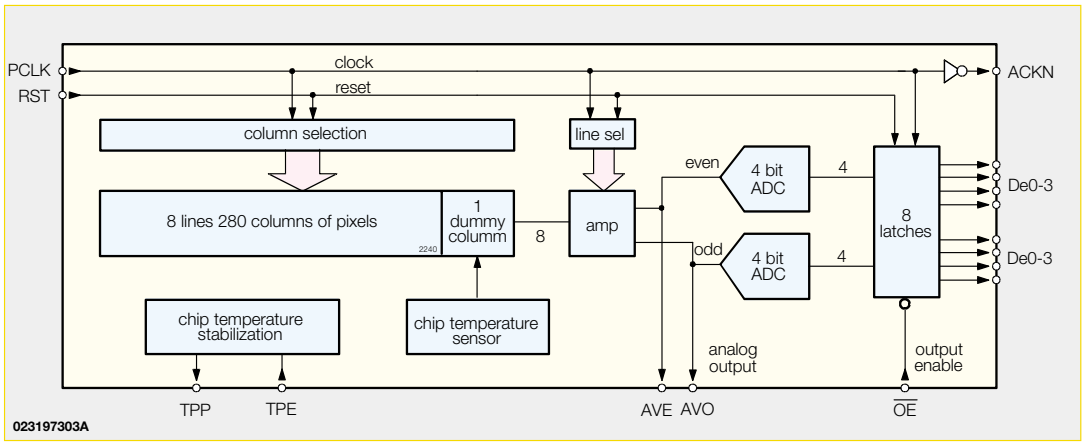

Bild 5: Interner Aufbau des Atmel-FingerChip

gen werden. Der Vorteil dabei ist, dass der Sensor bei jeder Erfassung automatisch gereinigt wird. Auch bei diesem Scan-Verfahren ist eine Auflösung von ca. 500 dpi zu erreichen.

Je nach mechanischer Konstruktion können verschiedene Bereiche eines Fingers gescannt werden. Während in Abbildung 4a nur die Papillarlinien der Fingerspitze erfasst werden, kann in Abbildung 4b und 4c ein wesentlich größerer Bereich zum späteren Vergleich dienen. Besonders beim Ablegen eines Referenzabdrucks sollte ein möglichst großer Ausschnitt des Fingers gescannt werden. Die besten Ergebnisse werden natürlich erzielt, wenn der Finger immer in der gleichen Position über den Sensor gezogen wird. Die interne Struktur des Atmel-Sensors zeigt Abbildung 5.

Auch bei diesem Sensor müssen mittels komplexer mathematischer Verfahren aus den Rohdaten des Fingerabdrucks die charakteristischen Merkmale herausgefiltert werden.

Sämtliche Funktionsblöcke für eine sichere und kostengünstige Erkennung von Fingerabdrücken hat die Firma Ikendi in einem ASIC integriert. Der Systemprogrammierer muss sich somit nicht mehr mit der recht komplexen Biometrie auseinander setzen. Das Ikendi Design-in-Kit mit dem Atmel-FingerChip ist in Abbildung 6 zu sehen. Neben dem Atmel-Zeilensensor kann die Ikendi Entwicklungsumgebung auch mit dem Infineon-FingerTip-Sensor arbeiten.

Nach der Verarbeitung der Rohdaten bleibt ein nur etwa 200 Byte großer Datensatz mit den charakteristischen Merkmalen übrig. Diese Daten werden dann vom ASIC in verschlüsselter Form ausgegeben.

Die Überprüfung eines Fingerabdrucks dauert bei diesem System weniger als 0,5 s.

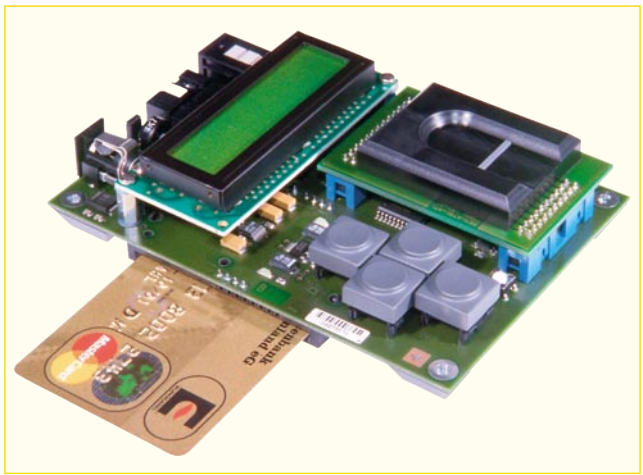

Bild 6: Ikendi Demo-Kit-Platine

Authen-Tec-Fingerprint-Sensoren

Einer der führenden Anbieter von Fingerprint-Sensoren ist die zu Harris gehörende amerikanische Firma Authen-Tec. Neben den Sensoren liefert auch Authen-Tec die komplette Systemtechnik.

Laut Herstellerangaben können mit Sensoren von Authen-Tec 99,99 % aller Fingerabdrücke erfasst werden, egal ob es sich um trockene, feuchte, verschmutzte, junge oder alte Haut handelt.

Die von Authen-Tec verwendete Trueprint-Technologie wertet das vom Finger erzeugte elektrische Feld aus. Dabei wird mit Hochfrequenz von 250 kHz bis 1 MHz gearbeitet und in tiefe Hautschichten eingedrungen. Im Vergleich zu optischen und kapazitiven Sensoren, die die Hautstruktur nur an der Oberfläche erfassen, werden bessere Ergebnisse erzielt, da oberflächliche Verletzungen und Verschmutzungen die Erfassung kaum beeinflussen.

Die Sensoren werden unter dem Produktnamen „FingerLoc" vertrieben und bestehen aus CMOS-Sensor-Arrays, die das elektrische Feld des zu erfassenden Fingers messen.

Angeboten werden unterschiedlich große Sensoren mit 128 x 128 Pixeln oder mit 96 x 96 Pixeln. Bei beiden Sensorvarianten ist die Auflösung von 250-1000 dpi einstellbar.

In Abbildung 7 ist der Sensor des Typs AF-S2 zu sehen, der aufgrund seiner großen Erfassungsfläche von 13 mm x 13 mm besonders gut für Zugangs-Kontrollsysteme, Sicherheitsanwendungen und Zeiterfassungssysteme geeignet ist. Der Sensor ist sehr robust und auch für den Außeneinsatz geeignet. Die gehärtete Sensoroberfläche ist besonders unempfindlich gegenüber Verkratzungen.

Mehr als 16000 Sensorelemente bilden dabei ein Antennen-Array zur Erfassung des elektrischen Feldes.

Untergebracht ist der komplette Baustein, dessen Arbeitstemperaturbereich von -20 °C bis +70 °C reicht, in einem 68-Pin-PLCC-Gehäuse mit den Abmessungen 24 x 24 x 3,5 mm.

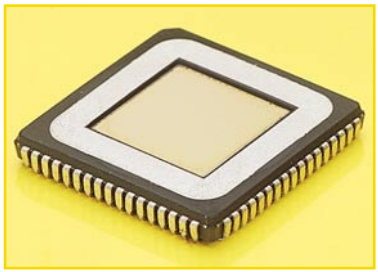

Bild 7: Der Authen-Tec-Sensor AF-S2 ist sehr robust und auch für Außenanwendungen geeignet

Für Anwendungen mit wenig Platz, wie z. B. in Laptops, steht der AIS 4000 (Abbildung 8) zur Verfügung. Dieser 20 x 20 mm große Baustein hat nur noch eine Dicke von 1,4 mm. Das Antennen-Array des AIS 4000, das unter der Produktbezeichnung Entré Pad vertrieben wird, besteht aus 96 x 96 Elementen. Für mobile Anwendungen wurde Wert auf eine geringe Leistungsaufnahme gelegt. So beträgt der Leis-

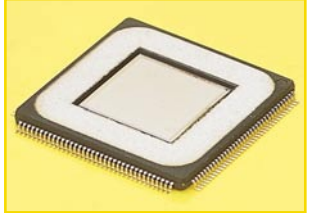

Bild 8: Für Anwendungen mit wenig Platz bietet sich der AIS 4000 mit einer Bauhöhe von nur 1,4 mm an.

tungsbedarf während der Erfassung 11 mW und im Standby-Mode werden dann nur noch 39,6 µW aufgenommen.

Ein weiterer Sensor befindet sich unter der Bezeichnung AIS 3500 in Vorbereitung. Die Erfassungsfläche beträgt dann nur noch 6,5 x 6,5 mm bei 128 x 128 Pixeln.

Bei allen ICs ist bereits die Verarbeitungslogik integriert. Für eine Standalone-Lösung werden neben dem Sensor noch ein Bildverarbeitungsprozessor und ein Mikrocontroller mit der entsprechenden Firmenware benötigt. Die entsprechenden Algorithmen zur Auswertung der Fingerprints werden ebenfalls von Authen-Tec zur Verfügung gestellt, sodass der Anwender sich nicht mit der komplizierten Biometrie befassen muss.

Die interne Struktur des FingerLoc-Sensors AF-S2 ist in Abbildung 9 zu sehen. Über ein Bussystem wird das Sensor-Array gesteuert und die erfassten Daten stehen dann über ein serielles Interface zur Verfügung. Bei 5 V Versorgungsspannung beträgt die Leistungsaufnahme des AF-S2 ca. 30 mW, während im Standby-Mode nur noch 100 µW benötigt werden.

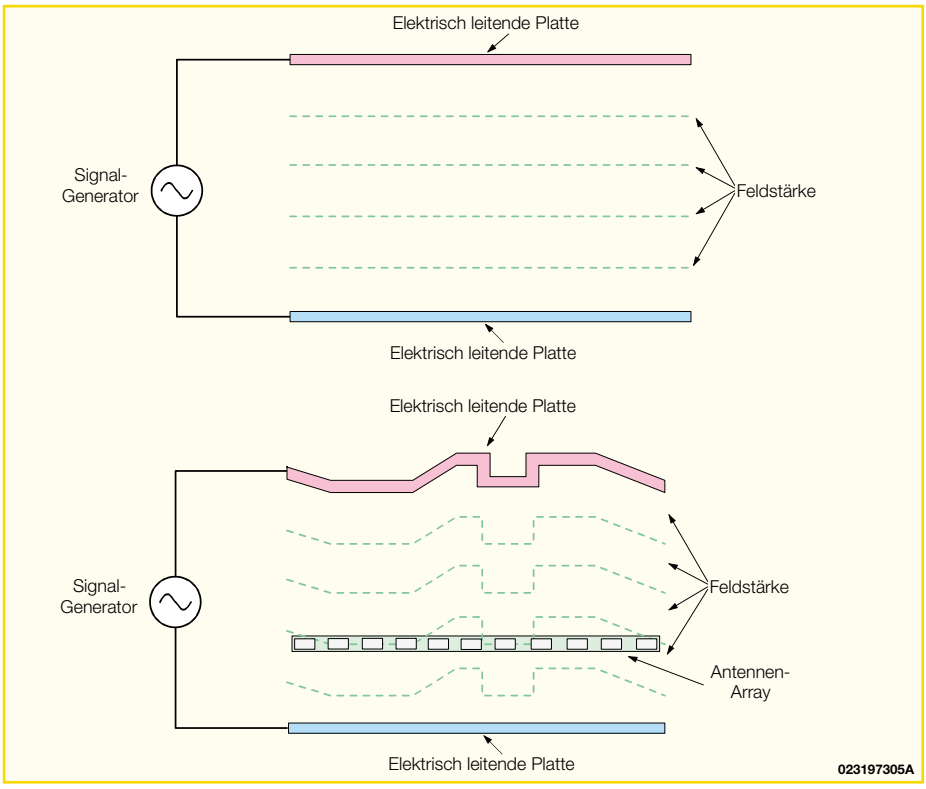

Bild 10: Grundprinzip der Authen-Tec Fingerprint-Sensoren.

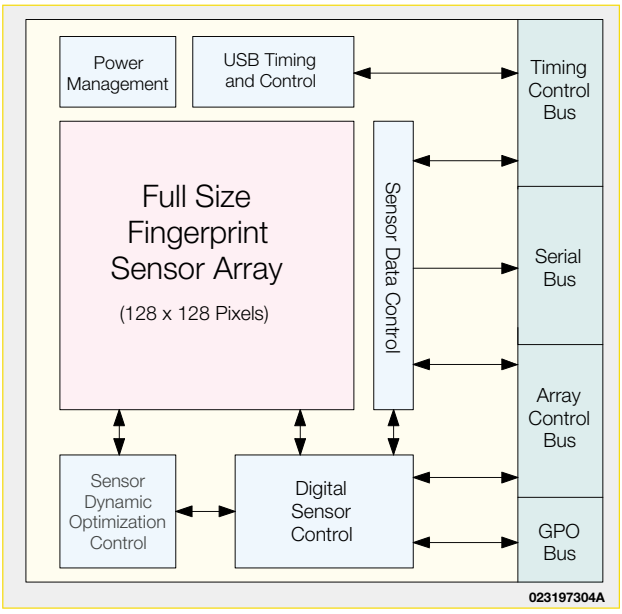

Bild 9: Interner Aufbau des Fingerprint-Sensors AF-S2

schen zwei leitenden Platten ist abhängig vom Abstand der Platten zueinander (Abbildung 10 oben). Wird die Form und somit der Abstand von einer Platte verändert, so ändert sich auch die Feldstärke zwischen den Platten entsprechend der Form, wie in Abbildung 10 unten skizziert ist.

Genau auf diesem Funktionsprinzip basiert die Funktionsweise der Authen Tec Fingerprint-Sensoren. Die obere Platte wird durch den zu erfassenden Finger ersetzt und die Hautstruktur bestimmt dann den Abstand der Platten zueinander. Abbildung 11 verdeutlicht dies mit einem Querschnitt durch die Haut des Fingers und des Sensors.

Der wesentliche Vorteil gegenüber optischen und kapazitiven Verfahren ist, dass nicht die tote Haut an der Oberfläche oder Verschmutzungen die „obere Platte" bilden, sondern die lebenden Hautzellen.

Die von den einzelnen Sensorelementen erfasste Feldstärke wird dann entsprechend den Verstärkern innerhalb des Fingerprint-Sensors zugeführt. Eine automatische Verstärkungsregelung sorgt für eine Anpassung an die jeweilige Beschaffenheit der Haut und den äußeren Erfassungsbedingungen. Durch die dynamische Anpassung der Verstärkung spielt es nahezu keine Rolle mehr, ob die zu erfassende Haut trocken, feucht oder verschmutzt ist.

Der Einsatz in Massenprodukten wie Laptops, PDAs usw. wird in naher Zukunft den Preis von Fingerprint-Sensoren sicherlich nach unten beeinflussen. ELV

Funktionsprinzip der Authen-Tec-Sensoren

Das Funktionsprinzip bei den Authen-Tec-Sensoren beruht, wie bereits erwähnt, auf die Messung des elektrischen Feldes. Die Stärke eines elektrischen Feldes zwi-

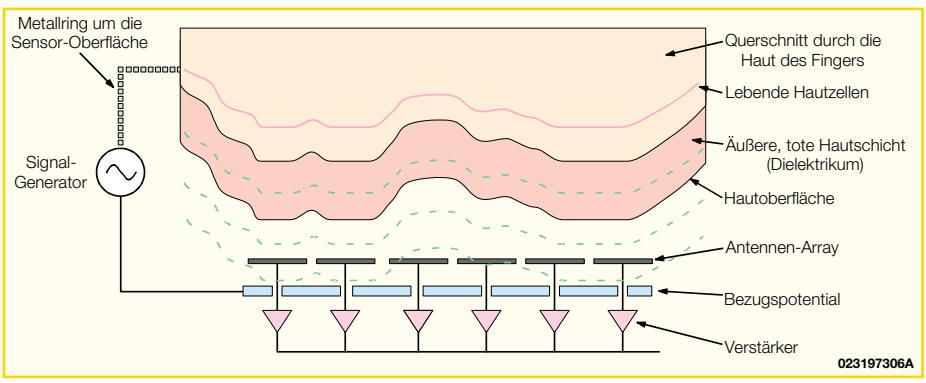

Bild 11: Ein Querschnitt durch die Haut eines Fingers verdeutlicht die Arbeitsweise.