A 500 DPI FINGERPRINT SENSOR IC IN CMOS TECHNOLOGY

Wolfgang PRIBYL, Siemens EZM Ges.m.b.H., Graz-Villach, Austria
Thomas SCHEITER, Siemens Semiconductor Division, Munich, Germany
Gerd HRIBERNIG, Siemens PSE, Graz, Austria

Keywords: biometrics, fingerprints, monolithic silicon sensor systems, CMOS, Complementary Metal Oxide Semiconductors, passwords, PIN codes, Personal Identification Number codes, security systems, identification systems, identification devices, authorization, pattern recognition, chip cards

Abstract: A monolithic fingerprint sensor has been implemented in a CMOS technology. This new sensor has a spatial resolution of 50 μm and translates the fingerprint pattern into a gray scale image of 256 x 256 pixels with 8 bit resolution. The sensor chip measures about 160 mm^2, together with a pattern recognition software, which extracts characteristic features, it forms a low cost system, which is well suited for a variety of applications as e.g. access control for buildings, computer networks and many other services.

CMOS integrirano vezje za senzor prstnih odtisov z ločljivostjo 500 dpi

Ključne besede: biometrika, odtisi prstni, sistemi senzorjev silicijevih monolitnih, CMOS polprevodniki kovinskooksidni komplementarni, gesla, PIN kode številčne identifikacijske osebne, sistemi varnostni, sistemi identifikacijski, naprave identifikacijske, odobritev, razpoznavanje vzorcev, chip kartice

Povzetek: Izdelali smo senzor prstnih odtisov v CMOS tehnologiji. Njegova prostorska ločljivost je 50 μm pri prevajanju oblike prstnega odtisa v sivo sliko velikosti 256x256 pik z 8 bitno ločljivostjo. Površina senzorskega vezja je 160 mm^2. Skupaj s programsko opremo za prepoznavanje oblik sestavlja sistem, katerega nizka cena omogoča različne uporabe, kot so nadzor vstopa v objekte, računalniške mreže in podobno.

1. Introduction

For a long time keys, made from metal in a more or less sophisticated way, have been a well accepted measure to protect property and the private sphere of people and organizations. But these keys can be stolen or lost, copying of the keys may reduce the security or privacy level to zero. Besides those well known key systems, which are based on the possession of a key also knowledge based systems are used. These systems substitute the physical keys by agreements of secret codes. Many of today's systems as e.g. mobile phones, credit cards, computers require special passwords or PIN-codes (personal identification number). The access to sensible areas of corporations and government agencies has to be restricted, but also electronic banking and electronic commerce in general need a proper identification and authorization, so that only the legitimate user may initiate transactions. If passwords and/or PIN codes are forgotten, the respective service is no longer available.

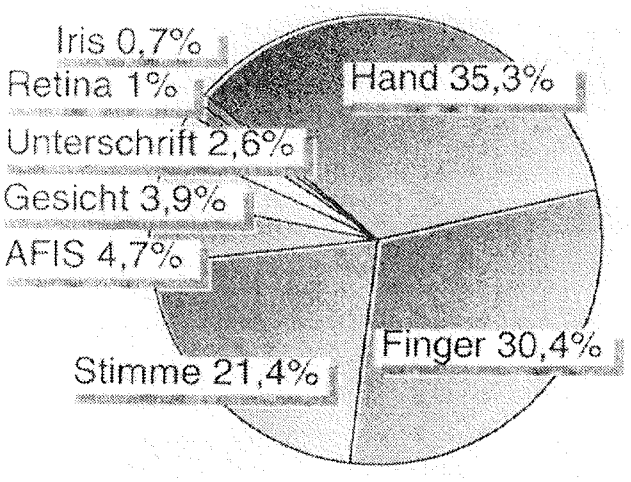

Fig.1: The global biometrics market, share of different systems

For the identification of the legitimate users biometric methods are best suited, which are based on constant features of the user's human body. Examples are the human speech, some characteristics of the face, the signature, structures of the human eye (pattern of the retina and iris) and many more. According to (Fig.1, /1/) most applications use pattern of the hand and fingers (65,7%) followed by voice recognition systems (21,4%). All other systems only have a small share of the overall biometrics market, either because of a high complexity of the systems needed, or because of the somehow invasive character of the measurement (e.g. illumination of the eye needed for the evaluation of the retina patterns). Simple, reliable and cheap systems are needed for the emerging security market for applications in PCs, telecommunication systems and electronic commerce applications.

2. The fingerprint as a unique characteristic of human beings

A typical fingerprint, covering an area of ca. 100 mm^2, shows about 12 characteristic positions, the so called minutia (Fig. 2). These minutia can be used as unique features for the identification of people. If compared to other methods, the fingerprint recognition systems offer several advantages:

- Since about 150 years the criminal science has carried out exhaustive theoretical and practical investigations on the use of fingerprints
- An almost infinite number of variations ($>>10^{22}$) enable the reliable and unique identification of all living people and even future generations
- The characteristics of the fingerprint do not change over the lifetime of a human being, even after most injuries the skin recovers in exactly the same pattern.
- The use of fingerprint identification systems is easy and pleasant, compared e.g. to systems based on the retina patterns and needing illumination and camera systems.

Fig. 2: Fingerprint record, features marked

The fingerprint recognition system described in this paper is based on the well established knowledge about the characteristics of fingerprints. The monolithic silicon sensor delivers a grayscale image and contains the significant characteristics (minutia) for each fingerprint, as e.g. ending lines, branching lines and characteristic turns and eddies. The features and characteristics and their relative position to each other are stored in a feature list. Such the overall memory needed can be reduced from 64 Kbytes for the whole gray scale image to a few hundreds of bytes for the still unique feature list. Due to this reduction, the whole system including a limited archive of legitimate users eventually will be implemented on a chip card.

If the system has to learn the features of a new person (enrollment procedure) several fingerprints have to be recorded and their respective features be stored in the feature list. Usually several fingers are stored at a time for each person, so that in case of an injury the access to the system is still possible. The available system can act in two different ways, depending on the planned application:

- Authentication: The person enters his/her ID, afterwards the system verifies the identity and rejects the access in the case of a mismatch.
- Identification: The system identifies the person based on the fingerprint presented and rejects all not previously stored persons.

Up to now the recording and the evaluation of finger prints was a costly procedure using very sophisticated equipment. With the availability of the monolithic „Fingertip-Sensor-System" it is now possible to record fingerprints very easily and to evaluate and identify the respective persons in a very short time. The whole process takes only a few seconds. Only if the extracted features correspond to the previously stored ones the protected device, system or transaction is released for the desired operation.

3. The Fingertip Sensor Chip - Hardware

A prototype of the sensor chip, fabricated in a 0,8 μm CMOS technology with 2 layers of metalization has been produced and evaluated; first product samples are shipped to the customers now. This is an important basis for a low cost mass production of fingerprint based identification and authorization systems. The sensor area consists of an array of 256 by 256 sensor electrodes with a grid of 50 μm and such cover an area of about 160 mm^2 with a spatial resolution of 500 dpi (dots per inch). The sensor electrodes are covered with a special dielectric layer, which protects the surface of the chip from the direct contact with the outside world. The finger has to touch the chip surface and depending on the local structure of ridges and valleys different capacitance values in the range of a few femtofarads (10^{-12} F) can be read out from the individual electrodes in the array. Such the information on the whole structure of the finger print is available as 65.536 coded capacitance values. A schematic cross section through the sensor array with a finger in contact can be seen in fig. 3, the block diagram of the whole sensor chip in fig.4. Besides the sensor array, the chip contains a direct analog-to-digital conversion of the capacitance values, a control unit based on a 1 MHz clock generator and an interface for the transmission of the gray scale image, which is coded as 8 bit/pixel.

For the prototypes a parallel interface for an easy connection to a PC has been chosen, later on standard interfaces for different microcontrollers or customized versions will be available. Fig. 5 shows a view of finished wafer of sensor chips with a finger applied.

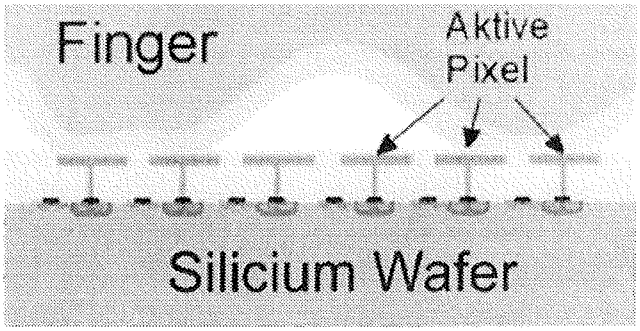

Fig. 3: Schematic cross section of sensor

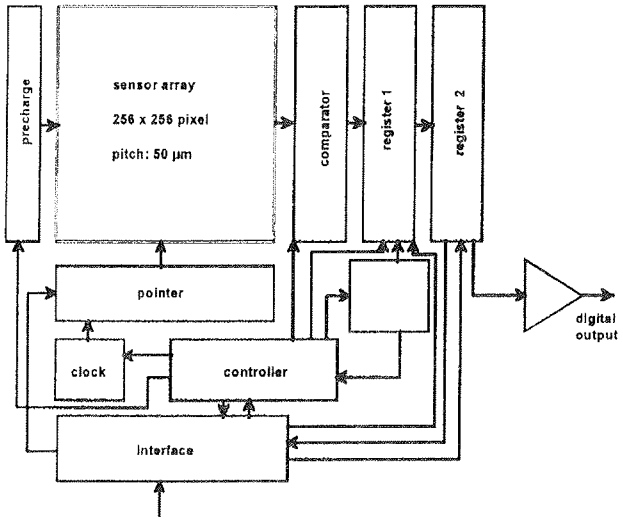

Fig. 4: Block diagram of the integrated finger print sensor.

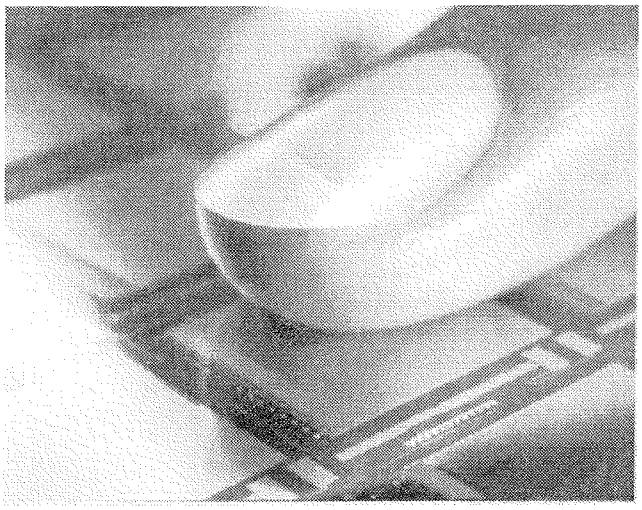

Fig. 5: Microphotograph of silicon sensor wafer with a finger applied

4. The Software for the Pattern Recognition Process

Since 1992 the PSE group in Graz is working on algorithms for the detection and identification of fingerprints. For this task conventional techniques of pattern recognition have been applied, in recent time new techniques as e.g. neural networks have been successfully applied. The software for this project has been developed within two years by a 5 person team. The processing chain (fig. 6) starts with the preprocessing of the sensor data and the transformation of these data into a normalized image. Then the identification of line structures, the completion of these lines and the extraction of the pure line structures is carried out. Then the characteristic features are extracted and classified using a neural

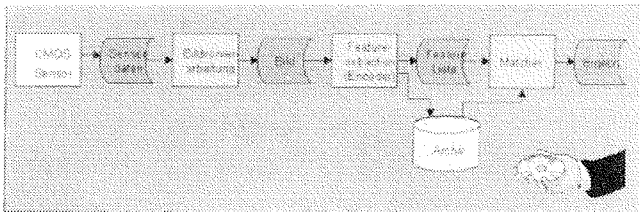

Fig. 6: Structure of software

network, the archive then stores only the result of these processes. When searching for a match later on, only the characteristic features are used. The compare algorithm is able to compensate for eventual translatorial or rotational changes in the pattern.

The recording and identification process for finger prints was a very complex procedure and requeired expensive instruments up to now. The new system can be used for a much broader range of applications, even in the low cost market segments. Almost every man - machine interface may use a fingerprint recognition system for increased security. The access to various types of computers, chipcards, immobilizer systems for vehicles, access control for buildings.

At the CeBit exhibition 1998 application examples have been demonstrated: a chip card incorporating a sensor, a prototype of a mobile phone and a PC keyboard (fig. 7, 8).

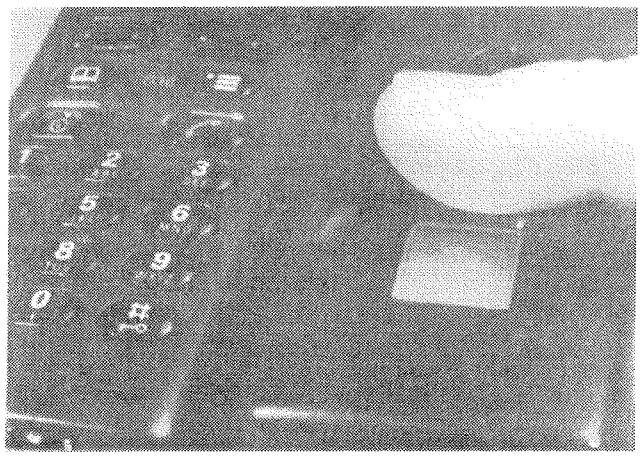

Fig. 7: Prototype of a GSM mobile phone with fingerprint authorization.

Literature:

/1/ Markt und Technik, volume 34/98

/2/ S.Jung, R.Thewes, T.Scheiter: CMOS Fingerprint Sensor with Automatic Local Contrast Adjustment and Pixel-Parallel Encoding Logic, submitted to the ISSCC'99, San Francisco, 2/99.

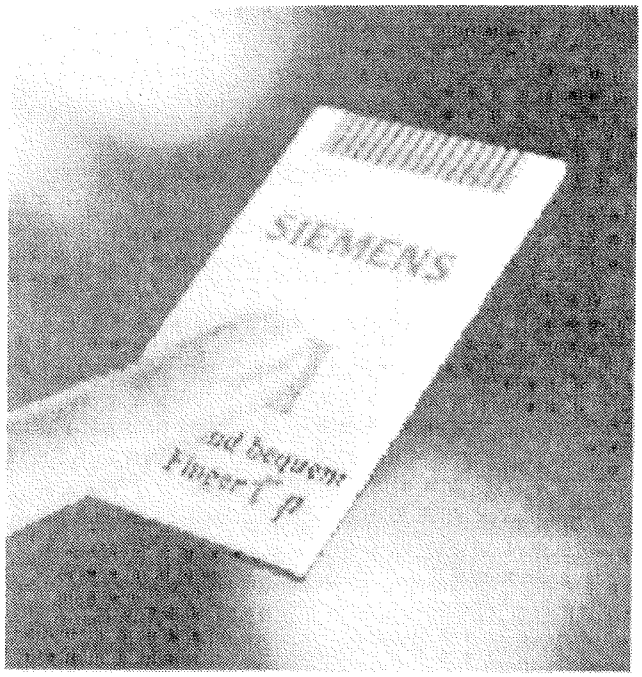

Fig. 8: Sample of a chip card with integrated fingerprint sensor

Dr. Wolfgang Pribyl
Siemens Entwicklungszentrum
für Mikroeelektronik GmbH
Hilmteichstr. 113
A-8043 Graz
Tel.: ++43 316 321210-10
Fax: ++ 316 32 1210-44
mailto: Wolfgang.Prybil@siemens-scg.com

Prispelo (Arrived): 16.9.1998 *Sprejeto (Accepted): 2.10.1998*