www.ijiarec.com

ISSN:2348-2079

Volume-5 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Finger print based vehicle starting system

Dharani.M(1), Karthiga.S(2), Gnanasekar(3)

Department of ECE

Shree venkateshwara hi-tech engineering college, gobi.

dharaniece2013@gmail.com

Abstract:-

Human identification is field very significant and which has undergone rap id changes with time. An important and very reliable human identification method is fingerprint identification. Fingerprint of every person is unique. So this helps in identifying a person or in improving security of a system.

In this paper we use a fingerprint module to read once identity to start the vehicle. For this we use a microcontroller to enable the ignition system if the matching between scanned data and the already existing data is correct. Comparison is done inside the finger print module itself and its output is given to microcontroller. Result is displayed in a LCD display whether the user is authorised or not .If the Scanned data is not matched message will be send to authorised user through GSM module.

In this project embedded system plays major role. It consist of Level converter, GSM, Finger Print sensor, Driver, Display and Power supply. Level converter is used to convert signal CMOSS to TTL and TTL to CMOSS. Fingerprint sensor is identifying the authorised user or not. It is connected to the Embedded system through Level converter. Vehicle connected to Embedded system through driver. Power supply is used to supply the system.

PROPOSED SYSTEM

This project efficiently defines the control of starting vehicle by using Finger Print method.This system discusses an Automatic Finger print identification for secure manner.The efficiency of the system is designed such that it can be used to control the theft.Thus fingerprint identification enhances the security of a vehicle and makes it possible only for some selected people to start the vehicle. Thus by implementing this relatively cheap and easily available system on a car one can ensure much greater security and exclusivity than that offered by a conventional lock and key.

OVERVIEW

The equipment is recogonized whether fingerprint belongs to user (or) the user (or) stranger.The user can record his/her fingerprint to the device manually at this stages of installment.Normally the engine starts through a small electric types inside the combustion chamber.These electric pulse can be controlled through internal relay.Once the relay are activated the required electric pulse is generated inside the combustion chamber.Fingerprint of the user is scanned through fingerprint scanner and store into the memory by converting them into binary values.These binary values are send to the PIC microcontroller for user recogonization. Level convector is used to remove unwanted signal of the fingerprint. The result of the PIC microcontroller are displayed through the LCD. The required for the operation is supplied with the help of power supplying unit. Once the result are positive the required signal are the send to the internal relay that produces necessary electric pulse for the ignition of engine. The connection and signals are transferred through where all electronic component are assembled together.

PIC MICROCONTROLLER

PIC is a family of Harvard architecture microcontrollers made by Microchip Technology, derived from the PIC1640 originally developed by General Instrument's Microelectronics Division. The name PIC initially referred to "Peripheral Interface Controller".

PICs are popular with developers and hobbyists alike due to their low cost, wide availability, large user base, extensive collection of application notes, availability of low cost or free development tools, and serial programming (and re-programming with flash memory) capability.

CORE ARCHITECTURE

The PIC architecture is distinctively minimalist. It is characterized by the following features:

- ✓ Separate code and data spaces (Harvard architecture)
- ✓ A small number of fixed length instructions
- ✓ Most instructions are single cycle execution (4 clock cycles), with single delay cycles upon branches and skips
- ✓ A single accumulator (W), the use of which (as source operand) is implied (i.e. is not encoded in the opcode)
- ✓ All RAM locations function as registers as both source and/or destination of math and other functions.
- ✓ A hardware stack for storing return addresses
- ✓ A fairly small amount of addressable data space (typically 256 bytes), extended through banking
- ✓ Data space mapped CPU, port, and peripheral registers
- ✓ The program counter is also mapped into the data space and writable (this is used to implement indirect jumps).
- ✓ Unlike most other CPUs, there is no distinction between memory space and register space because the RAM serves the job of both memory and registers and the RAM is usually just referred to as the register file or simply as the registers.

DATA SPACE (RAM)

PICs have a set of registers that function as general purpose RAM. Special purpose control registers for on-chip hardware resources are also mapped into the data space. The addressability of memory varies depending on device series, and all PIC devices have some banking mechanism to extend the addressing to additional memory. Later series of devices feature move instructions which can cover the whole addressable space, independent of the selected bank. In earlier devices (i.e., the baseline and mid-range cores), any register move had to be achieved via the accumulator.

To implement indirect addressing, a "file select register" (FSR) and "indirect register" (INDF) are used: A register number is written to the FSR, after which reads from or writes to INDF will actually be to or from the register pointed to by FSR. Later devices extended this concept with post- and pre- increment/decrement for greater efficiency in accessing sequentially stored data. This also allows FSR to be treated almost like a stack pointer.

External data memory is not directly addressable except in some high pin count PIC18 devices.

CODE SPACE

All PICs feature Harvard architecture, so the code space and the data space are separate. PIC code space is generally implemented as EPROM, ROM, or flash ROM.

In general, external code memory is not directly addressable due to the lack of an external memory interface. The exceptions are PIC17 and select high pin count PIC18 d0evices

WORD SIZE

The word size of PICs can be a source of confusion. All PICs handle (and address) data in 8-bit chunks, so they should be called 8-bit microcontrollers. However, the unit of addressability of the code space is not generally the same as the data space. For example, PICs in the baseline and mid-range families have program memory addressable in the same wordsize as the instruction width, ie. 12 or 14 bits respectively. In contrast, in the PIC18 series, the program memory is addressed in 8-bit increments (bytes), which differ from the instruction width of 16 bits.

In order to be clear, the program memory capacity is usually stated in number of (single word) instructions, rather than in bytes.

STACKS

PICs have a hardware call stack, which is used to save return addresses. The hardware stack is not software accessible on earlier devices, but this changed with the 18 series devices.

Hardware support for a general purpose parameter stack was lacking in early series, but this greatly improved in the 18 series, making the 18 series architecture more friendly to high level language compilers.

INSTRUCTION SET

A PIC's instructions vary from about 35 instructions for the low-end PICs to over 80 instructions for the high-end PICs. The instruction set includes instructions to perform a variety of operations on registers directly, the accumulator and a literal constant or the accumulator and a register, as well as for conditional execution, and program branching.

Some operations, such as bit setting and testing, can be performed on any numbered register, but bi-operand arithmetic operations always involve W; writing the result back to either W or the other operand register. To load a constant, it is necessary to load it into W before it can be moved into another register. On the older cores, all register moves needed to pass through W, but this changed on the "high end" cores.

PIC cores have skip instructions which are used for conditional execution and branching. The skip instructions are: 'skip if bit set', and, 'skip if bit not set'. Because cores before PIC18 had only unconditional branch instructions, conditional jumps are implemented by a conditional skip (with the opposite condition) followed by an unconditional branch. Skips are also of utility for conditional execution of any immediate single following instruction.

The PIC architecture has no (or very meager) hardware support for automatically saving processor state when servicing

interrupts. The 18 series improved this situation by implementing shadow registers which save several important registers during an interrupt.

IN GENERAL, PIC INSTRUCTIONS FALL INTO 5 CLASSES:

Operation on W with 8-bit immediate ("literal") operand. E.g. movlw (move literal to W), andlw (AND literal with W). One instruction peculiar to the PIC is retlw, load immediate into W and return, which is used with computed branches to produce lookup tables.

Operation with W and indexed register. The result can be written to either the W register (e.g. addwf reg,w). or the selected register (e.g. addwf reg,f).

Bit operations. These take a register number and a bit number, and perform one of 4 actions: set or clear a bit, and test and skip on set/clear. The latter are used to perform conditional branches. The usual ALU status flags are available in a numbered register so operations such as "branch on carry clear" are possible.

Control transfers. Other than the skip instructions previously mentioned, there are only two: goto and call.

A few miscellaneous zero-operand instructions, such as return from subroutine, and sleep to enter low-power mode.

PERFORMANCE

Many of these architectural decisions are directed at the maximization of top-end speed, or more precisely of speed-to-cost ratio. The PIC architecture was among the first scalar CPU designs, and is still among the simplest and cheapest. The Harvard architecture - in which instructions and data come from conveniently separate sources - simplifies timing and microcircuit design greatly, and this pays benefits in areas like clock speed, price, and power consumption.

The PIC is particularly suited to implementation of fast lookup tables in the program space. Such lookups are O(1) and can complete via a single instruction taking two instruction cycles. Basically any function can be modelled in this way. Such optimization is facilitated by the relatively large program space of the PIC (e.g. 4096 x 14-bit words on the 16F690) and by the design of the instruction set, which allows for embedded constants.

The simplicity of the PIC, and its scalar nature, also serve to greatly simplify the construction of real-time code. It is typically possible to multiply the line count of a PIC assembler listing by the instruction cycle time to determine execution time. (This is true because skip-based instructions take 2 cycles whether the skip occurs or doesn't.) On other CPUs (even the Atmel, with its MUL instruction), such quick methods are just not possible. In low-level development, precise timing is often critical to the success of the application, and the real-time features of the PIC can save crucial engineering time.

A similarly useful and unique property of PICs is that their interrupt latency is constant (it's also low: 3 instruction cycles). The delay is constant even though instructions can take one or two instruction cycles: a dead cycle is optionally inserted into the interrupt response sequence to make this true. External interrupts have to be synchronized with the four clock instruction cycle, otherwise there can be a one instruction cycle jitter. Internal interrupts are already synchronized.

The constant interrupt latency allows PICs to achieve interrupt driven low jitter timing sequences. An example of this is a video sync pulse generator. Other microcontrollers can do this in some cases, but it's awkward. The non-interrupt code has to anticipate the interrupt and enter into a sleep state before it arrives. On PICs, there is no need for this.

The three-cycle latency is increased in practice because the PIC does not store its registers when entering the interrupt routine. Typically, 4 instructions are needed to store the W-register, the status register and switch to a specific bank before starting the actual interrupt processing.

LIMITATIONS

The PIC architectures have several limitations:

- ✓ Only a single accumulator
- ✓ A small instruction set
- ✓ Operations and registers are not orthogonal; some instructions can address RAM and/or immediate constants, while others can only use the accumulator
- ✓ Memory must be directly referenced in arithmetic and logic operations, although indirect addressing is available via 2 additional registers
- ✓ Register-bank switching is required to access the entire RAM of many devices, making position-independent code complex and inefficient
- ✓ Conditional skip instructions are used instead of conditional jump instructions used by most other architectures
- ✓ The following limitations have been addressed in the PIC18, but still apply to earlier cores:
- ✓ Indexed addressing mode is very rudimentary

STACK:

The hardware call stack is so small that program structure must often be flattened

The hardware call stack is not addressable, so pre-emptive task switching cannot be implemented

Software-implemented stacks are not efficient, so it is difficult to generate reentrant code and support local variables

Program memory is not directly addressable, and thus space-inefficient and/or time-consuming to access. (This is true of most Harvard architecture microcontrollers.)

With paged program memory, there are two page sizes to worry about: one for CALL and GOTO and another for computed GOTO (typically used for table lookups). For example, on PIC16, CALL and GOTO have 11 bits of addressing, so the page size is 2KB. For computed GOTOs, where you add to PCL, the page size is 256 bytes. In both cases, the upper address bits are provided by the PCLATH register. This register must be changed every time control transfers between pages. PCLATH must also be preserved by any interrupt handler.[5]

Compiler development

These properties have made it difficult to develop compilers that target PIC microcontrollers. While several commercial compilers are available, in 2008, Microchip finally released their C compilers, C18, and C30 for their line of 18f 24f and 30/33f processors. By contrast, Atmel's AVR microcontrollers—which are competitive with PIC in terms of hardware capabilities and price, but feature a RISC instruction set—have long been supported by the GNU C Compiler.

Also, because of these properties, PIC assembly language code can be difficult to comprehend. Judicious use of simple macros can make PIC assembly language much more palatable, but at the cost of a reduction in performance. For example, the original Parallax PIC assembler "pasm" has macros which hide W and make the PIC look like a two-address machine. It has macro instructions like "mov b,a" (move the data from address a to address b) and "add b,a" (add data from address a to data in address b). It also hides the skip instructions by providing three operand branch macro instructions such as "cjne a, b, dest" (compare a with b and jump to dest if they are not equal).

Family Core Architectural Differences

Baseline Core Devices

These devices feature a 12-bit wide code memory, a 32-byte register file, and a tiny two level deep call stack. They are represented by the PIC10 series, as well as by some PIC12 and PIC16 devices. Baseline devices are available in 6-pin to 40-pin packages.

Generally the first 7 to 9 bytes of the register file are special-purpose registers, and the remaining bytes are general purpose RAM. If banked RAM is implemented, the bank number is selected by the high 3 bits of the FSR. This affects register numbers 16–31; registers 0–15 are global and not affected by the bank select bits.

The ROM address space is 512 words (12 bits each), which may be extended to 2048 words by banking. CALL and GOTO instructions specify the low 9 bits of the new code location; additional high-order bits are taken from the staus register. Note that a CALL instruction only includes 8 bits of address, and may only specify addresses in the first half of each 512-word page.

The instruction set is as follows. Register numbers are referred to as "f", while constants are referred to as "k". Bit numbers (0–7) are selected by "b". The "d" bit selects the destination: 0 indicates W, while 1 indicates that the result is written back to source register f.

12-bit PIC instruction set

Opcode (binary)	Mnemonic	Description
0000 0000 0000	NOP	No operation
0000 0000 0010	OPTION	Load OPTION register with contents of W
0000 0000 0011	SLEEP	Go into standby mode
0000 0000 0100	CLRWDT	Reset watchdog timer
0000 0000 01ff	TRIS f	Move W to port control register (f=1..3)
0000 001 fffff	MOVWF f	Move W to f
0000 010 xxxxx	CLRW	Clear W to 0 (a.k.a CLR x,W)
0000 011 fffff	CLRF f	Clear f to 0 (a.k.a. CLR f,F)
0000 10d fffff	SUBWF f,d	Subtract W from f (d = f − W)
0000 11d fffff	DECF f,d	Decrement f (d = f − 1)
0001 00d fffff	IORWF f,d	Inclusive OR W with F (d = f OR W)

0001 01d fffff	ANDWF f,d	AND W with F (d = f AND W)
0001 10d fffff	XORWF f,d	Exclusive OR W with F (d = f XOR W)
0001 11d fffff	ADDWF f,d	Add W with F (d = f + W)
0010 00d fffff	MOVF f,d	Move F (d = f)
0010 01d fffff	COMF f,d	Complement f (d = NOT f)
0010 10d fffff	INCF f,d	Increment f (d = f + 1)
0010 11d fffff	DECFSZ f,d	Decrement f (d = f − 1) and skip if zero
0011 00d fffff	RRF f,d	Rotate right F (rotate right through carry)
0011 01d fffff	RLF f,d	Rotate left F (rotate left through carry)
0011 10d fffff	SWAPF f,d	Swap 4-bit halves of f (d = f<<4 | f>>4)
0011 11d fffff	INCFSZ f,d	Increment f (d = f + 1) and skip if zero
0100 bbb fffff	BCF f,b	Bit clear f (Clear bit b of f)
0101 bbb fffff	BSF f,b	Bit set f (Set bit b of f)
0110 bbb fffff	BTFSC f,b	Bit test f, skip if clear (Test bit b of f)
0111 bbb fffff	BTFSS f,b	Bit test f, skip if set (Test bit b of f)
1000 kkkkkkkk	RETLW k	Set W to k and return
1001 kkkkkkkk	CALL k	Save return address, load PC with k
101 kkkkkkkkk	GOTO k	Jump to address k (9 bits!)
1100 kkkkkkkk	MOVLW k	Move literal to W (W = k)
1101 kkkkkkkk	IORLW k	Inclusive or literal with W (W = k OR W)
1110 kkkkkkkk	ANDLW k	AND literal with W (W = k AND W)
1111 kkkkkkkk	XORLW k	Exclusive or literal with W (W = k XOR W)

Mid-Range Core Devices

These devices feature a 14-bit wide code memory, and an improved 8 level deep call stack. The instruction set differs very little from the baseline devices, but the increased opcode width allows 128 registers and 2048 words of code to be directly addressed. The mid-range core is available in the majority of devices labeled PIC12 and PIC16.

The first 32 bytes of the register space are allocated to special-purpose registers; the remaining 96 bytes are used for general-purpose RAM. If banked RAM is used, the high 16 registers (0x70–0x7F) are global, as are a few of the most important special-purpose registers, including the STATUS register which holds the RAM bank select bits. (The other global registers are FSR and INDF, the low 8 bits of the program counter PCL, the PC high preload register PCLATH, and the master interrupt control register INTCON.)

The PCLATH register supplies high-order instruction address bits when the 8 bits supplied by a write to the PCL register, or the 11 bits supplied by a GOTO or CALL instruction, is not sufficient to address the available ROM space.

PIC24 and dsPIC 16-bit Microcontrollers

In 2001, Microchip introduced the dsPIC series of chips[6], which entered mass production in late 2004. They are Microchip's first inherently 16-bit microcontrollers. PIC24 devices are designed as general purpose microcontrollers. dsPIC devices include digital signal processing capabilities in addition.

Architecturally, although they share the PIC moniker, they are very different from the 8-bit PICs. The most notable differences are

- ✓ they feature a set of 16 working registers
- ✓ they fully support a stack in RAM, and do not have a hardware stack
- ✓ bank switching is not required to access RAM or special function registers
- ✓ data stored in program memory can be accessed directly using a feature called Program Space Visibility
- ✓ interrupt sources may be assigned to distinct handlers using an interrupt vector table
- ✓ Some features are:
- ✓ hardware MAC (multiply-accumulate)
- ✓ barrel shifting
- ✓ bit reversal
- ✓ (16×16)-bit multiplication and other DSP operations.
- ✓ hardware support for loop indexing

DIRECT MEMORY ACCESS

dsPICs can be programmed in C using a variant of gcc.

PIC32 32-bit Microcontrollers

In November 2007 Microchip introduced the new PIC32MX family of 32-bit microcontrollers. The initial device line-up is based on the industry standard MIPS32 M4K Core[5]. The device can be programmed using the Microchip MPLAB C Compiler for PIC32 MCUs, a variant of the GCC compiler. The first 18 models currently in production (PIC32MX3xx and PIC32MX4xx) are pin to pin compatible and share the same peripherals set with the PIC24FxxGA0xx family of (16-bit) devices allowing the use of common libraries, software and hardware tools.

The PIC32 architecture brings a number of new features to Microchip portfolio, including:

- The highest execution speed 80 MIPS (90+ Dhrystone MIPS @80MHz)
- The largest FLASH memory: 512kbyte
- One instruction per clock cycle execution
- The first cached processor
- Allows execution from RAM
- Full Speed Host/Dual Role and OTG USB capabilities
- Full JTAG and 2 wire programming and debugging
- Real-time trace
- Device Variants and Hardware Features

PIC devices generally feature:

- Sleep mode (power savings).
- Watchdog timer.
- Various crystal or RC oscillator configurations, or an external clock.
- Variants
- Within a series, there are still many device variants depending on what hardware resources the chip features.
- General purpose I/O pins.
- Internal clock oscillators.
- 8/16/32 Bit Timers.
- Internal EEPROM Memory.
- Synchronous/Asynchronous Serial Interface USART.
- MSSP Peripheral for I²C and SPI Communications.
- Capture/Compare and PWM modules.
- Analog-to-digital converters (up to ~1.0 MHz).
- USB, Ethernet, CAN interfacing support.
- External memory interface.
- Integrated analog RF front ends (PIC16F639, and rfPIC).
- KEELOQ Rolling code encryption peripheral (encode/decode)
- And many more.

Trends

The first generation of PICs with EPROM storage are almost completely replaced by chips with Flash memory. Likewise, the original 12-bit instruction set of the PIC1650 and its direct descendants has been superseded by 14-bit and 16-bit instruction sets. Microchip still sells OTP (one-time-programmable) and windowed (UV-erasable) versions of some of its EPROM based PICs for legacy support or volume orders. It should be noted that the Microchip website lists PICs that are not electrically erasable as OTP despite the fact that UV erasable windowed versions of these chips can be ordered.

Development Tools

Commercially Supported

Microchip provides a freeware IDE package called MPLAB, which includes an assembler, linker, software simulator, and debugger. They also sell C compilers for the PIC18 and dsPIC which integrate cleanly with MPLAB. Free student versions of the C compilers are also available with all features. But for the free versions, optimizations will be disabled after 60 days.[8]

Several third parties make C,[9] BASIC[10] and Pascal[11] language compilers for PICs, many of which integrate to MPLAB and/or feature their own IDE.

A blockset for Matlab/Simulink allow one to generate C and binary files from a simulink model. Most common peripherals have their blocksets and you do not need to write the configuration code.

Open Source

The following development tools are available for the PIC family under the GPL or other free software or open sources licenses.

FreeRTOS is a mini real time kernel ported to PIC18, PIC24, dsPIC and PIC32 architectures.

GPUTILS is free and available from the GPUTILS website.

GPSIM is an Open Source simulator for the PIC microcontrollers featuring hardware modules that simulate specific devices that might be connected to them, like LCDs.

SDCC supports 8-bit PIC micro controllers (PIC16, PIC18). Currently, throughout the SDCC website, the words, "Work is in progress", is frequently used to describe the status of SDCC's support for PICs.

KTechlab, an OpenSource microcontroller IDE written in c++ and qt. Ktechlab supports the programming of microcontrollers using C, Assembly, Microbe (a BASIC-like language) and using flowcode a graphical programming language similar to Flowcode

Ktechlab is a free IDE for programming PIC Microcontroller. It allows one to write the program in C, Assembly, Microbe (a BASIC-like language) and using FlowChart Method.

PiKdev runs on Linux and is a simple graphic IDE for the development of PIC-based applications. It currently supports assembly language. Non Open Source C language is also supported for PIC 18 devices. PiKdev is developed in C++ under Linux and is based on the KDE environment.

Piklab is a forked version of PiKdev and is managed as SourceForge Project. Piklab adds to Pikdev by providing support for programmers and debuggers. Currently, Piklab supports the JDM, PIC Elmer, K8048, HOODMICRO, ICD1, ICD2, PICkit1, PICKkit2, and PicStart+ as programming devices and has debugging support for ICD2 in addition to using the simulator, GPSim.

JAL stands for Just another Language. It is a Pascal-like language that is easily mastered. The compiler supports a few Microchip (16c84, 16f84, 12c508, 12c509, 16F877) and SX microcontrollers. The resulting assembly language can then be viewed, modified and further processed as if you were programming directly in assembler.

PMP (Pic Micro Pascal) is a free Pascal language compiler and IDE. It is intended to work with Microchip MPLAB that it uses device definition files, assembler and linker. It supports PIC10 to PIC18 devices.

The GNU Compiler Collection and the GNU Binutils have been ported to the PIC24, dsPIC30F and dsPIC33F in the form of Microchip's MPLAB C30 compiler and MPLAB ASM30 Assembler.

MIOS is a real-time operating system written in PIC assembly, optimized for MIDI processing and other musical control applications. There is a C wrapper for higher level development. Currently it runs on the MIDIbox Hardware Platform.

FlashForth is a native Forth operating system for the PIC18F and the dsPIC30F series. It makes the PIC a standalone computer with an interpreter, compiler, assembler and multitasker.

Great Cow Basic (GCBasic) The syntax of Great Cow BASIC is based on that of QBASIC/FreeBASIC. The assembly code produced by Great Cow BASIC can be assembled and run on almost all 10, 12, 16 and 18 series PIC chips.

POWER SUPPLIES

INTRODUCTION:

The present chapter introduces the operation of power supply circuits built using filters, rectifiers, and then voltage regulators. Starting with an ac voltage, a steady dc voltage is obtained by rectifying the ac voltage, then filtering to a dc level, and finally, regulating to obtain a desired fixed dc voltage. The regulation is usually obtained from an IC voltage regulator unit, which takes a dc voltage and provides a somewhat lower dc voltage, which remains the same even if the input dc voltage varies, or the output load connected to the dc voltage changes.

A block diagram containing the parts of a typical power supply and the voltage at various points in the unit is shown in fig 19.1. The ac voltage, typically 120 V rms, is connected to a transformer, which steps that ac voltage down to the level for the desired dc output. A diode rectifier then provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation. A regulator circuit can use this dc input to provide a dc voltage that not only has much less ripple voltage but also remains the same dc value even if the input dc voltage varies somewhat, or the load connected to the output dc voltage changes. This voltage regulation is usually obtained using one of a number of popular voltage regulator IC units.

IC VOLTAGE REGULATORS:

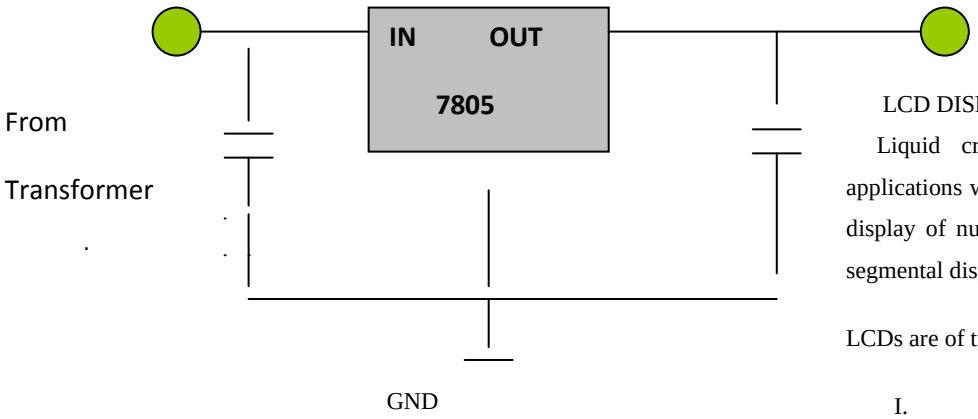
Voltage regulators comprise a class of widely used ICs. Regulator IC units contain the circuitry for reference source, comparator amplifier, control device, and overload protection all in a single IC. Although the internal construction of the IC is somewhat different from that described for discrete voltage regulator circuits, the external operation is much the same. IC units provide regulation of either a fixed positive voltage, a fixed negative voltage, or an adjustably set voltage.

A power supply can be built using a transformer connected to the ac supply line to step the ac voltage to a desired amplitude, then rectifying that ac voltage, filtering with a capacitor and RC filter, if desired, and finally regulating the dc voltage using an IC regulator. The regulators can be selected for operation with load currents from hundreds of milli amperes to tens of amperes, corresponding to power ratings from milliwatts to tens of watts.

THREE-TERMINAL VOLTAGE REGULATORS:

Fig shows the basic connection of a three-terminal voltage regulator IC to a load. The fixed voltage regulator has an unregulated dc input voltage, Vi, applied to one input terminal, a regulated output dc voltage, Vo, from a second terminal, with the third terminal connected to ground. For a selected regulator, IC device specifications list a voltage range over which the input voltage can vary to maintain a regulated output voltage over a range of load current. The specifications also list the amount of output voltage change resulting from a change in load current (load regulation) or in input voltage (line regulation).

Fixed Positive Voltage Regulators:



The series 78 regulators provide fixed regulated voltages from 5 to 24 V. Figure 19.26 shows how one such IC, a 7812, is connected to provide voltage regulation with output from this unit of +12V dc. An unregulated input voltage Vi is filtered by capacitor C1 and connected to the IC's IN terminal. The IC's OUT terminal provides a regulated + 12V which is filtered by capacitor C2 (mostly for any high-frequency noise). The third IC terminal is connected to ground (GND). While the input voltage may vary over some permissible voltage range, and the output load may vary over some acceptable range, the output voltage remains constant within specified voltage variation limits. These limitations are spelled out in the manufacturer's specification sheets. A table of positive voltage regulated ICs is provided in table 19.1.

TABLE 19.1 Positive Voltage Regulators in 7800 series

IC Part	Output Voltage (V)	Minimum Vi (V)
7805	+5	7.3
7806	+6	8.3
7808	+8	10.5
7810	+10	12.5
7812	+12	14.6
7815	+15	17.7
7818	+18	21.0
7824	+24	27.1

LCD DISPLAY:

Liquid crystal cell displays (LCDs) are used in similar applications where LEDs are used. These applications are display of display of numeric and alphanumeric characters in dot matrix and segmental displays.

LCDs are of two types:

I. Dynamic scattering type
II. Field effect type

The construction of a dynamic scattering liquid crystal cell. The liquid crystal material may be one of the several components, which exhibit optical properties of a crystal though they remain in liquid form. Liquid crystal is layered between glass sheets with transparent electrodes deposited on the inside faces.

When a potential is applied across the cell, charge carriers flowing through the liquid disrupt the molecular alignment and produce turbulence. When the liquid is not activated, it is transparent. When the liquid is activated the molecular turbulence causes light to be scattered in all directions and the cell appease to be bright.

This phenomenon is called dynamic scattering.

The construction of a field effect liquid crystal display is similar to that of the dynamic scattering type, with the exception that two thin polarizing optical filters are placed at the inside of each glass sheet. The liquid crystal material in the field effect cell is also of different type from employed in the dynamic scattering cell. The material used is twisted nemayic type and actually twists the light passing through the cell when the latter is not energised.

Liquid crystal cells are of two types:

i. Transmittive type

ii. Reflective type

In the transmittive type cell, both glass sheets are transparent, so that light from a rear source is scattered in the forward direction when the cell is activated.

In reflective type cell has a reflecting surface on one side of glass sheets. The incident light on the front surface of the cell is dynamically scattered by an activated cell. Both types of cells appear quite bright when activated even under ambient light conditions.

The liquid crystals are light reflectors are transmitters and therefore they consume small amounts of energy (unlike light generators).

The seven segment display, the current is about 25micro Amps for dynamic scattering cells and 300micro amps for field effect cells. Unlike LEDs which can work on d.c. the LCDs require a.c. voltage supply. A typical voltage supply to dynamic scattering LCD is 30v peak to peak with 50 Hz

PIN DESCRIPTION

PIN NO	SYMBOL	FUNCTION
1	Vss	Ground terminal of Module
2	Vdd	Supply terminal of Module, + 5v
3	Vo	Power supply for liquid crystal drive
4	RS	Register select RS=0…Instruction register RS=1…Data register
5	R/W	Read/Write R/W=1…Read R/W=0…Write
6	E(EI)	Enable
7-14	DB0-DB7	Bi-directional Data Bus. Data Transfer is performed once ,thru DB0-DB7,incase of interface data length is 8-bits;and twice, thru DB4-DB7 in the case of interface data length is 4-bits.Upper four bits first then lower four bits.
15	LAMP-(L-)	LED or EL lamp power supply terminals
16	LAMP+(L+) (E2)	Enable

ADVANTAGES:

1. Consume much lesser energy (i.e. low power) when compared to LEDs.
2. Utilizes the light available outside and no generation of light.
3. Since very thin layer of liquid crystal is used, more suitable to act as display elements (in digital watches, pocket calculators, ect.)
4. Since reflectivity is highly sensitive to temperature, used as temperature measuring sensor.
5. Very cheap.

DISADVANTAGES:

1. Angle of viewing is very limited.
2. External light is a must for display.

3. Since not generating its own light and makes use of external light for display, contrast is poor.

4. Cannot be used under wide range of temperature.

APPLICATIONS:

1. Watches

2. Fax & Copy machines & Calculators.

FINGERPRINT SENSOR

A **fingerprint** in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human hand. A print from the foot can also leave an impression of friction ridges. A friction ridge is a raised portion of the epidermis on the fingers and toes (digits), the palm of the hand or the sole of the foot, consisting of one or more connected ridge units of friction ridge skin. These are sometimes known as "epidermal ridges" which are caused by the underlying interface between the dermal papillae of the dermis and the interpapillary (rete) pegs of the epidermis. These epidermal ridges serve to amplify vibrations triggered, for example, when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. These ridges also assist in gripping rough surfaces, as well as smooth wet surfaces.

Impressions of fingerprints may be left behind on a surface by the natural secretions of sweat from the eccrine glands that are present in friction ridge skin, or they may be made by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

Fingerprints used for identification

Fingerprint identification, known as dactyloscopy or hand print identification, is the process of comparing two instances of friction ridge skin impressions (see Minutiae), from human fingers, the palm of the hand or even toes, to determine whether these impressions could have come from the same individual. The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike in every detail; even two impressions recorded immediately after each other from the same hand. Fingerprint identification, also referred to as individualization, involves an expert, or an expert computer system operating under threshold scoring rules, determining whether two friction ridge impressions are likely to have originated from the same finger or palm (or toe or sole).

An intentional recording of friction ridges is usually made with black printer's ink rolled across a contrasting white background, typically a white card. Friction ridges can also be recorded digitally using a technique called Live Scan. A "latent print" is the chance recording of friction ridges deposited on the surface of an object or a wall. Latent prints are invisible to the naked eye, whereas "patent prints" or "plastic prints" are viewable with the un-aided eye. Latent prints are often fragmentary and require chemical methods, powder, or alternative light sources in order to be made clear. Sometimes an ordinary bright flashlight will make a latent print visible.

When friction ridges come into contact with a surface that will take a print, material that is on the friction ridges such as perspiration, oil, grease, ink or blood, will be transferred to the surface. Factors which affect the quality of friction ridge impressions are numerous. Pliability of the skin, deposition pressure, slippage, the material from which the surface is made, the roughness of the surface and the substance deposited are just some of the various factors which can cause a latent print to appear differently from any known recording of the same friction ridges. Indeed, the conditions surrounding every instance of friction ridge deposition are unique and never duplicated. For these reasons, fingerprint examiners are required to undergo extensive training. The scientific study of fingerprints is called dermatoglyphics.

Fingerprint types

Exemplar prints

Exemplar prints, or known prints, is the name given to fingerprints deliberately collected from a subject, whether for purposes of enrollment in a system or when under arrest for a suspected criminal offense. During criminal arrests, a set of exemplar prints will normally include one print taken from each finger that has been rolled from one edge of the nail to the other, plain (or slap) impressions of each of the four fingers of each hand, and plain impressions of each thumb. Exemplar prints can be collected using Live Scan or by using ink on paper cards.

Latent prints

Although the word latent means hidden or invisible, in modern usage for forensic science the term latent prints means any chance or accidental impression left by friction ridge skin on a surface, regardless of whether it is visible or invisible at the time of deposition. Electronic, chemical and physical processing techniques permit visualization of invisible latent print residues whether they are from natural sweat on the skin or from a contaminant such as motor oil, blood, ink, paint or some other form of dirt. The different types of fingerprint patterns, such as arch, loop and whorl, will be described below.

Latent prints may exhibit only a small portion of the surface of a finger and this may be smudged, distorted, overlapped by other prints from the same or from different individuals, or any or all of these in combination. For this reason, latent prints usually present an “inevitable source of error in making comparisons,” as they generally “contain less clarity, less content, and less undistorted information than a fingerprint taken under controlled conditions, and much, much less detail compared to the actual patterns of ridges and grooves of a finger.

Patent prints

Patent prints are chance friction ridge impressions which are obvious to the human eye and which have been caused by the transfer of foreign material from a finger onto a surface. Some obvious examples would be impressions from flour and wet clay. Because they are already visible and have no need of enhancement they are generally photographed rather than being lifted in the way that latent prints are. An attempt to preserve the actual print is always made for later presentation in court, and there are many techniques used to do this. Patent prints can be left on a surface by materials such as ink, dirt, or blood.

Plastic prints

A plastic print is a friction ridge impression left in a material that retains the shape of the ridge detail. Although very few criminals would be careless enough to leave their prints in a lump of wet clay, this would make a perfect plastic print. Commonly encountered examples are melted candle wax, putty removed from the perimeter

of window panes and thick grease deposits on car parts. Such prints are already visible and need no enhancement, but investigators must not overlook the potential that invisible latent prints deposited by accomplices may also be on such surfaces. After photographically recording such prints, attempts should be made to develop other non-plastic impressions deposited from sweat or other contaminants.

Electronic recording

There has been a newspaper report of a man selling stolen watches sending images of them on a mobile phone, and those images included parts of his hands in enough detail for police to be able to identify fingerprint patterns.

Classifying fingerprints

Before computerisation replaced manual filing systems in large fingerprint operations, manual fingerprint classification systems were used to categorize fingerprints based on general ridge formations (such as the presence or absence of circular patterns on various fingers), thus permitting filing and retrieval of paper records in large collections based on friction ridge patterns alone. The most popular ten-print classification systems include the Roscher system, the Juan Vucetich system, and the Henry Classification System. Of these systems, the Roscher system was developed in Germany and implemented in both Germany and Japan, the Vucetich system (developed by a Croatian-born Buenos Aires Police Officer) was developed in Argentina and implemented throughout South America, and the Henry system was developed in India and implemented in most English-speaking countries.

In the Henry system of classification, there are three basic fingerprint patterns: loop, whorl and arch, which constitute 60–65%, 30–35% and 5% of all fingerprints respectively. There are also more complex classification systems that break down patterns even further, into plain arches or tented arches, and into loops that may be radial or ulnar, depending on the side of the hand toward which the tail points. Ulnar loops start on the pinky-side of the finger, the side closer to the ulna, the lower arm bone. Radial loops start on the thumb-side of the finger, the side closer to the radius. Whorls may also have sub-group classifications including plain whorls, accidental whorls, double loop whorls, peacock's eye, composite, and central pocket loop whorls.

Other common fingerprint patterns include the tented arch, the plain arch, and the central pocket loop.

The system used by most experts, although complex, is similar to the Henry System of Classification. It consists of five fractions, in which R stands for right, L for left, i for index finger, m for middle finger, t for thumb, r for ring finger and p(pinky) for little finger. The fractions are as follows: Ri/Rt + Rr/Rm + Lt/Rp + Lm/Li + Lp/Lr. The numbers assigned to each print are based on whether or not they are whorls. A whorl in the first fraction is given a 16, the second an 8, the third a 4, the fourth a 2, and 0 to the last fraction. Arches and loops are assingned values of 0. Lastly, the numbers in the numerator and denominator are added up, using the scheme:

$$(Ri + Rr + Lt + Lm + Lp)/(Rt + Rm + Rp + Li + Lr)$$

and a 1 is added to both top and bottom, to exclude any possibility of division by zero. For example, if the right ring finger and the left index finger have whorls, the fractions would look like this:

0/0 + 8/0 + 0/0 + 0/2 + 0/0 + 1/1, and the calculation: (0 + 8 + 0 + 0 + 0 + 1)/(0 + 0 + 0 + 2 + 0 + 1) = 9/3 = 3.

Using this system reduces the number of prints that the print in question needs to be compared to. For example, the above set of prints would only need to be compared to other sets of fingerprints with a value of 3.

Arch

Loop

(Right Loop)

Whorl

Arch
(Tented Arch)

Footprints

Friction ridge skin present on the soles of the feet and toes (plantar surfaces) is as unique in its ridge detail as are the fingers and palms (palmar surfaces). When recovered at crime scenes or on items of evidence, sole and toe impressions can be used in the same manner as finger and palm prints to effect identifications. Footprint (toe and sole friction ridge skin) evidence has been admitted in courts in the United States since 1934.

The footprints of infants, along with the thumb or index finger prints of mothers, are still commonly recorded in hospitals to assist in verifying the identity of infants. Often, the only identifiable ridge detail that can be seen on a baby's foot is from the large toe or adjacent to the large toe.

It is not uncommon for military records of flight personnel to include bare foot inked impressions. Friction ridge skin protected inside flight boots tends to survive the trauma of a plane crash (and accompanying fire) better than fingers. Even though the US Armed Forces DNA Identification Laboratory (AFDIL), as of 2010, stored refrigerated DNA samples from all active duty and reserve personnel, almost all casualty identifications are effected using fingerprints from military ID card records (live scan fingerprints are recorded at the time such cards are issued). When friction ridge skin is not available from military personnel's remains, DNA and dental records are used to confirm identity.

Fingerprint capture and detection

Livescan devices

A fingerprint scanner

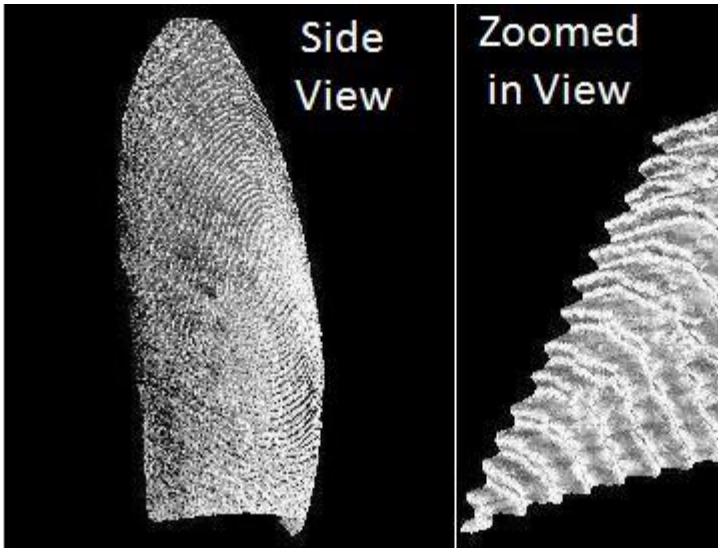
Fingerprint being scanned

Fingerprint image acquisition is considered to be the most critical step in an automated fingerprint authentication system, as it determines the final fingerprint image quality, which has a drastic effect on the overall system performance. There are different types of fingerprint readers on the market, but the basic idea behind each is to measure the physical difference between ridges and valleys.

A fingerprint reader on a laptop

All the proposed methods can be grouped into two major families: solid-state fingerprint readers and optical fingerprint readers. The

procedure for capturing a fingerprint using a sensor consists of rolling or touching with the finger onto a sensing area, which according to the physical principle in use (optical, ultrasonic, capacitive or thermal) captures the difference between valleys and ridges. When a finger touches or rolls onto a surface, the elastic skin deforms. The quantity and direction of the pressure applied by the user, the skin conditions and the projection of an irregular 3D object (the finger) onto a 2D flat plane introduce distortions, noise and inconsistencies in the captured fingerprint image. These problems result in inconsistent, irreproducible and non-uniform irregularities in the image During each acquisition, therefore, the results of the imaging are different and uncontrollable. The representation of the same fingerprint changes every time the finger is placed on the sensor plate, increasing the complexity of any attempt to match fingerprints, impairing the system performance and consequently, limiting the widespread use of this biometric technology.



3D fingerprint

In order to overcome these problems, as of 2010, non-contact or touch less 3D fingerprint scanners have been developed. Acquiring detailed 3D information, 3D fingerprint scanners take a digital approach to the analog process of pressing or rolling the finger. By modeling the distance between neighboring points, the fingerprint can be imaged at a resolution high enough to record all the necessary detail. **Latent fingerprint detection**

Since the late nineteenth century, fingerprint identification methods have been used by police agencies around the world to identify suspected criminals as well as the victims of crime. The basis of the traditional fingerprinting technique is simple. The skin on the palmar surface of the hands and feet forms ridges, so-called papillary ridges, in patterns that are unique to each individual and which do not change over time. Even identical twins (who share their DNA) do not have identical fingerprints. The best way to render latent fingerprints visible, so that they can be photographed, can be complex and may depend, for example, on the type of surfaces on which they have been left. It is generally necessary to use a 'developer', usually a powder or chemical reagent, to produce a high degree of visual contrast between the ridge patterns and the surface on which a fingerprint has been deposited.

Developing agents depend on the presence of organic materials or inorganic salts for their effectiveness, although the water deposited may also take a key role. Fingerprints are typically formed from the aqueous-based secretions of the eccrine glands of the fingers and palms with additional material from sebaceous glands primarily from the forehead. This latter contamination results from the common human behaviors of touching the face and hair. The resulting latent fingerprints consist usually of a substantial proportion of water with small traces of amino acids and chlorides mixed with a fatty, sebaceous component which contains a number of fatty acids and triglycerides. Detection of a small proportion of reactive organic substances such as urea and amino acids is far from easy.

Fingerprints at a crime scene may be detected by simple powders, or by chemicals applied in situ. More complex techniques, usually involving chemicals, can be applied in specialist laboratories to appropriate articles removed from a crime scene. With advances in these more sophisticated techniques, some of the more advanced crime scene investigation services from around the world were, as of 2010, reporting that 50% or more of the fingerprints recovered from a crime scene had been identified as a result of laboratory-based techniques.

Laboratory techniques

Although there are hundreds of reported techniques for fingerprint detection, many of these are only of academic interest and there are only around 20 really effective methods which are currently in use in the more advanced fingerprint laboratories around the world. Some of these techniques, such as ninhydrin, diazafluorenone and vacuum metal deposition, show great sensitivity and are used operationally. Some fingerprint reagents are specific, for example ninhydrin or diazafluorenone reacting with amino acids. Others such as ethyl cyanoacrylate polymerisation, work apparently by water-based catalysis and polymer growth. Vacuum metal deposition using gold and zinc has been shown to be non-specific, but can detect fat layers as thin as one molecule. More mundane methods, such as the application of fine powders, work by adhesion to sebaceous deposits and possibly aqueous deposits in the case of fresh fingerprints. The aqueous component of a fingerprint, whilst initially sometimes making up over 90% of the weight of the fingerprint, can evaporate quite quickly and may have mostly gone after 24 hours. Following work on the use of argon ion lasers for fingerprint detection, a wide

range of fluorescence techniques have been introduced, primarily for the enhancement of chemically-developed fingerprints; the inherent fluorescence of some latent fingerprints may also be detected. The most comprehensive manual of the operational methods of fingerprint enhancement is published by the UK Home Office Scientific Development Branch and is used widely around the world.

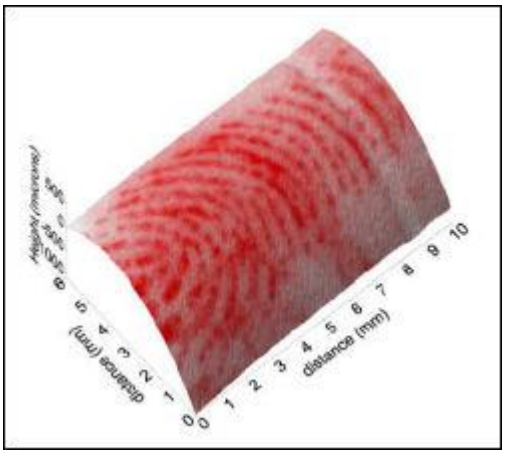
Research

The International Fingerprint Research Group (IFRG) which meets biennially, consists of members of the leading fingerprint research groups from Europe, the US, Canada, Australia and Israel and leads the way in the development, assessment and implementation of new techniques for operational fingerprint detection.

One problem for the early twenty-first century is the fact that the organic component of any deposited material is readily destroyed by heat, such as occurs when a gun is fired or a bomb is detonated, when the temperature may reach as high as 500°C. Encouragingly, however, the non-volatile inorganic component of eccrine secretion has been shown to remain intact even when exposed to temperatures as high as 600°C.

A technique has been developed that enables fingerprints to be visualised on metallic and electrically conductive surfaces without the need to develop the prints first. This technique involves the use of an instrument called a scanning Kelvin probe (SKP), which measures the voltage, or electrical potential, at pre-set intervals over the surface of an object on which a fingerprint may have been deposited. These measurements can then be mapped to produce an image of the fingerprint. A higher resolution image can be obtained by increasing the number of points sampled, but at the expense of the time taken for the process. A sampling frequency of 20 points per mm is high enough to visualise a fingerprint in sufficient detail for identification purposes and produces a voltage map in 2–3 hours. As of 2010, this technique had been shown to work effectively on a wide range of forensically important metal surfaces including iron, steel and aluminium. While initial experiments were performed on flat surfaces, the technique has been further developed to cope with irregular or curved surfaces, such as the warped cylindrical surface of fired cartridge cases. Research during 2010 at Swansea University has found that physically removing a fingerprint from a metal surface, for example by rubbing with a tissue, does not necessarily result in the loss of all fingerprint information from that surface. The reason for this is that the differences in potential that are the basis of the visualisation are caused by the interaction of inorganic salts in the fingerprint deposit and the metal surface and begin to occur as soon as the finger comes into contact with the metal, resulting in the formation of metal-ion complexes that cannot easily be removed.

Cartridge case with an applied fingerprint



Scanning Kelvin probe scan of the same cartridge case with the fingerprint detected. The Kelvin probe can easily cope with the 3D curvature of the cartridge case, increasing the versatility of the technique.

Another problem for the early twenty-first century is that during crime scene investigations, a decision has to be made at an early stage whether to attempt to retrieve fingerprints through the use of developers or whether to swab surfaces in an attempt to salvage material for DNA profiling. The two processes are mutually incompatible, as fingerprint developers destroy material that could potentially be used for DNA analysis, and swabbing is likely to make fingerprint identification impossible.

The application of the new scanning Kelvin probe (SKP) fingerprinting technique, which makes no physical contact with the fingerprint and does not require the use of developers, has the potential to allow fingerprints to be recorded whilst still leaving intact material that could subsequently be subjected to DNA analysis. A forensically usable prototype was under development at Swansea University during 2010, in research that was generating significant interest from the British Home Office and a number of different

police forces across the UK, as well as internationally. The hope is that this instrument could eventually be manufactured in sufficiently large numbers to be widely used by forensic teams worldwide.[22][23]

The disappearance of children's latent prints

In 1995, researchers at the Oak Ridge National Laboratory, at the instigation of Detective Art Bohanan of the Knoxville Police Department, discovered that children's fingerprints are considerably more short-lived than adult fingerprints. The rapid disappearance of children's fingerprints was attributed to a lack of the more waxy oils that become present at the onset of puberty. The lighter fatty acids of children's fingerprints evaporate within a few hours. As of 2010, researchers at Oak Ridge National Laboratory are investigating techniques to capture these lost fingerprints.

Fingerprints reveal drug use

The secretions, skin oils and dead cells in a human fingerprint contain residues of various chemicals and their metabolites present in the body. These can be detected and used for forensic purposes. For example, the fingerprints of tobacco smokers contain traces of cotinine, a nicotine metabolite; they also contain traces of nicotine itself. Caution should be used, as its presence may be caused by mere contact of the finger with a tobacco product. By treating the fingerprint with gold nanoparticles with attached cotinine antibodies, and then subsequently with a fluorescent agent attached to cotinine antibodies, the fingerprint of a smoker becomes fluorescent; non-smokers' fingerprints stay dark. The same approach, as of 2010, is being tested for use in identifying heavy coffee drinkers, cannabis smokers, and users of various other drugs.[24][25] In 2008, British researchers developed methods of identifying users of marijuana, cocaine and methadone from their fingerprint residues.

United States databases and compression

In the United States, the FBI manages a fingerprint identification system and database called the Integrated Automated Fingerprint Identification System, or IAFIS, which currently holds the fingerprints and criminal records of over 51 million criminal record subjects and over 1.5 million civil (non-criminal) fingerprint records. US Visit currently holds a repository of the fingerprints of over 50 million people, primarily in the form of two-finger records. In 2008, US Visit hoped to have changed over to a system recording FBI-standard ten-print records.

Most American law enforcement agencies use Wavelet Scalar Quantization (WSQ), a wavelet-based system for efficient storage of compressed fingerprint images at 500 pixels per inch (ppi). WSQ was developed by the FBI, the Los Alamos National Lab, and the National Institute for Standards and Technology (NIST). For fingerprints recorded at 1000 ppi spatial resolution, law enforcement (including the FBI) uses JPEG 2000 instead of WSQ.

History

Antiquity and the medieval period

Fingerprints have been found on ancient Babylonian clay tablets, seals, and pottery. We have also been found on the walls of Egyptian tombs and on Minoan, Greek, and Chinese pottery, as well as on bricks and tiles from ancient Babylon and Rome. Some of these fingerprints were deposited unintentionally by the potters and masons as a natural consequence of their work, and others were made in the process of adding decoration. However, on some pottery, fingerprints have been impressed so deeply into the clay that they were possibly intended to serve as an identifying mark by the maker.

Fingerprints were used as signatures in ancient Babylon in the second millennium BCE. In order to protect against forgery, parties to a legal contract would impress their fingerprints into a clay tablet on which the contract had been written. By 246 BCE, Chinese officials were impressing their fingerprints into the clay seals used to seal documents. With the advent of silk and paper in China, parties to a legal contract impressed their handprints on the document. Sometime before 851 CE, an Arab merchant in China, Abu Zayd Hasan, witnessed Chinese merchants using fingerprints to authenticate loans. By 702, Japan had adopted the Chinese practice of sealing contracts with fingerprints.

Although ancient peoples probably did not realize that fingerprints could uniquely identify individuals, references from the age of the Babylonian king Hammurabi (1792-1750 BCE) indicate that law officials would take the fingerprints of people who had been arrested. During China's Qin Dynasty, records have shown that officials took hand prints, foot prints as well as finger prints as evidence from a crime scene. In China, around 300 CE, handprints were used as evidence in a trial for theft. By 650, the Chinese historian Kia Kung-Yen remarked that fingerprints could be used as a means of authentication. In his Jami al-Tawarikh (Universal History), the Persian physician Rashid-al-Din Hamadani (also known as "Rashideddin", 1247–1318) refers to the Chinese practice of identifying people via their fingerprints, commenting: "Experience shows that no two individuals have fingers exactly alike. In Persia at

this time, government documents may have been authenticated with thumbprints.

Europe in the 17th and 18th centuries

In 1684, the English physician, botanist, and microscopes Nehemiah Grew (1641–1712) published the first scientific paper to describe the ridge structure of the skin covering the fingers and palms. In 1685, the Dutch physician Govard Bidloo (1649–1713) and the Italian physician Marcello Malpighi (1628–1694) published books on anatomy which also illustrated the ridge structure of the fingers. A century later, in 1788, the German anatomist Johann Christoph Andreas Mayer (1747–1801) recognized that fingerprints are unique to each individual.

Modern era

Jan Evangelista Purkyně or Purkinje (1787–1869), a Czech physiologist and professor of anatomy at the University of Breslau, published a thesis in 1823 discussing 9 fingerprint patterns, but he did not mention any possibility of using fingerprints to identify people. Some years later, the German anatomist Georg von Meissner (1829–1905) studied friction ridges, and five years after this, in 1858, Sir William James Herschel initiated fingerprinting in India. In 1877 at Hooghly (near Calcutta) he instituted the use of fingerprints on contracts and deeds to prevent the then-rampant repudiation of signatures and he registered government pensioners' fingerprints to prevent the collection of money by relatives after a pensioner's death. Herschel also fingerprinted prisoners upon sentencing to prevent various frauds that were attempted in order to avoid serving a prison sentence.

In 1880, Dr Henry Faulds, a Scottish surgeon in a Tokyo hospital, published his first paper on the subject in the scientific journal Nature, discussing the usefulness of fingerprints for identification and proposing a method to record them with printing ink. He also established their first classification and was also the first to identify fingerprints left on a vial. Returning to the UK in 1886, he offered the concept to the Metropolitan Police in London but it was dismissed at that time. Faulds wrote to Charles Darwin with a description of his method but, too old and ill to work on it, Darwin gave the information to his cousin, Francis Galton, who was interested in anthropology. Having been thus inspired to study fingerprints for ten years, Galton published a detailed statistical model of fingerprint analysis and identification and encouraged its use in forensic science in his book Finger Prints. He had calculated that the chance of a "false positive" (two different individuals having the same fingerprints) was about 1 in 64 billion

Juan Vucetich, an Argentine chief police officer, created the first method of recording the fingerprints of individuals on file, associating these fingerprints to the anthropometric system of Alphonse Bertillon, who had created, in 1879, a system to identify individuals by anthropometric photographs and associated quantitative descriptions. In 1892, after studying Galton's pattern types, Vucetich set up the world's first fingerprint bureau. In that same year, Francisca Rojas of Necochea, was found in a house with neck injuries, whilst her two sons were found dead with their throats cut. Rojas accused a neighbour, but despite brutal interrogation, this neighbour would not confess to the crimes. Inspector Alvarez, a colleague of Vucetich, went to the scene and found a bloody thumb mark on a door. When it was compared with Rojas' prints, it was found to be identical with her right thumb. She then confessed to the murder of her sons.

A Fingerprint Bureau was established in Calcutta (Kolkata), India, in 1897, after the Council of the Governor General approved a committee report that fingerprints should be used for the classification of criminal records. Working in the Calcutta Anthropometric Bureau, before it became the Fingerprint Bureau, were Azizul Haque and Hem Chandra Bose. Haque and Bose were Indian fingerprint experts who have been credited with the primary development of a fingerprint classification system eventually named after their supervisor, Sir Edward Richard Henry. The Henry Classification System, co-devised by Haque and Bose, was accepted in England and Wales when the first United Kingdom Fingerprint Bureau was founded in Scotland Yard, the Metropolitan Police headquarters, London, in 1901. Sir Edward Richard Henry subsequently achieved improvements in dactyloscopy.

In the United States, Dr Henry P. DeForrest used fingerprinting in the New York Civil Service in 1902, and by 1906, New York City Police Department Deputy Commissioner Joseph A. Faurot, an expert in the Bertillon system and a finger print advocate at Police Headquarters, introduced the fingerprinting of criminals to the United States.

The Scheffer case of 1902 is the first case of the identification, arrest and conviction of a murderer based upon fingerprint evidence. Alphonse Bertillon identified the thief and murderer Scheffer, who had previously been arrested and his fingerprints filed some months before, from the fingerprints found on a fractured glass showcase, after a theft in a dentist's apartment where the dentist's employee was found dead. It was able to be proved in Court that the fingerprints had been made after the showcase was broken. A year later, Alphonse Bertillon created a method of getting fingerprints off smooth surfaces and took a further step in the advance of dactyloscopy.

Validity of fingerprinting for identification

The validity of forensic fingerprint evidence has been challenged by academics, judges and the media. While fingerprint identification was an improvement on earlier anthropometric systems, the subjective nature of matching, despite a very low error rate, has made this forensic practice controversial.

Certain specific criticisms are now being accepted by some leaders of the forensic fingerprint community, providing an incentive to improve training and procedures.

Criticism

The words "reliability" and "validity" have specific meanings to the scientific community. Reliability means that successive tests bring the same results. Validity means that these results are judged to accurately reflect the external criteria being measured.

"Although experts are often more comfortable relying on their instincts, this reliance does not always translate into superior predictive ability. For example, in the popular Analysis, Comparison, Evaluation, and Verification (ACE-V) paradigm for fingerprint identification, the verification stage, in which a second examiner confirms the assessment of the original examiner, may increase the consistency of the assessments. But while the verification stage has implications for the reliability of latent print comparisons, it does not assure their validity."

The few tests that have been made of the validity of forensic fingerprinting have not been supportive of the method.

"Despite the absence of objective standards, scientific validation, and adequate statistical studies, a natural question to ask is how well fingerprint examiners actually perform. Proficiency tests do not validate a procedure per se, but they can provide some insight into error rates. In 1995, the Collaborative Testing Service (CTS) administered a proficiency test that, for the first time, was “designed, assembled, and reviewed” by the International Association for Identification (IAI).The results were disappointing. Four suspect cards with prints of all ten fingers were provided together with seven latents. Of 156 people taking the test, only 68 (44%) correctly classified all seven latents. Overall, the tests contained a total of 48 incorrect identifications. David Grieve, the editor of the Journal of Forensic Identification, describes the reaction of the forensic community to the results of the CTS test as ranging from “shock to disbelief,” and added:

'Errors of this magnitude within a discipline singularly admired and respected for its touted absolute certainty as an identification process have produced chilling and mind- numbing realities. Thirty-four participants, an incredible 22% of those involved, substituted presumed but false certainty for truth. By any measure, this represents a profile of practice that is unacceptable and thus demands positive action by the entire community.'

What is striking about these comments is that they do not come from a critic of the fingerprint community, but from the editor of one of its premier publications."

—Sandy L Zabell, 2005

Investigations have been conducted into whether experts can objectively focus on feature information in fingerprints without being misled by extraneous information, such as context. Fingerprints that have previously been examined and assessed by latent print experts to make a positive identification of suspects have then been re-presented to those same experts in a new context which makes it likely that there will be no match. Within this new context, most of the fingerprint experts made different judgments, thus contradicting their own previous identification decisions.

Complaints have been made that there have been no published, peer-reviewed studies directly examining the extent to which people can correctly match fingerprints to one another Experiments have been carried out using naïve undergraduates to match images of fingerprints. The results of these experiments demonstrate that people can identify fingerprints quite well, and that matching accuracy can vary as a function of both source finger type and image similarity.

Defense

Fingerprints collected at a crime scene, or on items of evidence from a crime, have been used in forensic science to identify suspects, victims and other persons who touched a surface. Fingerprint identification emerged as an important system within police agencies in the late 19th century, when it replaced anthropometric measurements as a more reliable method for identifying persons having a prior record, often under a false name, in a criminal record repository The science of fingerprint identification has been able to assert its standing amongst forensic sciences for many reasons.

Track record

Fingerprinting has served all governments worldwide during the past 100 years or so to provide accurate identification of criminals. No two fingerprints have ever been found identical in many billions of human and automated computer comparisons. Fingerprints are the fundamental tool for the identification of people with a criminal

history in every police agency It remains the most commonly gathered forensic evidence worldwide and in most jurisdictions fingerprint examination outnumbers all other forensic examination casework combined. Moreover, it continues to expand as the premier method for identifying persons, with tens of thousands of people added to fingerprint repositories daily in America alone — far more than other forensic databases.

Professional standing and certification

Fingerprinting was the basis upon which the first forensic professional organization was formed, the International Association for Identification (IAI), in 1915. The first professional certification program for forensic scientists was established in 1977, the IAI's Certified Latent Print Examiner program, which issued certificates to those meeting stringent criteria and had the power to revoke certification where an individual's performance warranted it Other forensic disciplines have followed suit and established their own certification programs.

Instances of error

Brandon Mayfield and the Madrid bombing

Brandon Mayfield is an Oregon lawyer who was identified as a participant in the 2004 Madrid train bombings based on a fingerprint match by the FBI. The FBI Latent Print Unit processed a fingerprint collected in Madrid and reported a "100 percent positive" match against one of the 20 fingerprint candidates returned in a search response from their IAFIS — Integrated Automated Fingerprint Identification System. The FBI initially called it an "absolutely incontrovertible match". Subsequently, however, Spanish National Police examiners suggested that the print did not match Mayfield and after two weeks, identified another man whom they claimed the fingerprint did belong to. The FBI acknowledged their error, and a judge released Mayfield, who had spent two weeks in police custody, in May 2004 In January 2006, a U.S. Justice Department report was released which criticized the FBI for sloppy work but exonerated them of some more serious allegations. The report found that the misidentification had been due to a misapplication of methodology by the examiners involved: Mayfield is an American-born convert to Islam and his wife is an Egyptian immigrant but these are not factors that should have affected fingerprint search technology.

On 29 November 2006, the FBI agreed to pay Brandon Mayfield US$2 million in compensation. The judicial settlement allowed Mayfield to continue a suit regarding certain other government practices surrounding his arrest and detention. The formal apology stated that the FBI, which erroneously linked him to the 2004 Madrid bombing through a fingerprinting mistake, had taken steps to "ensure that what happened to Mr Mayfield and the Mayfield family does not happen again."

René Ramón Sánchez

René Ramón Sánchez, a legal Dominican Republic immigrant to the US was arrested on July 15, 1995, on a charge of driving while intoxicated (Driving Under the Influence, or DUI). His fingerprints, however, were placed on a card containing the name, Social Security number and other data for one Leo Rosario, who was being processed at the same time. Leo Rosario had been arrested for selling cocaine to an undercover police officer. On October 11, 2000, while returning from a visit to relatives in the Dominican Republic, René was mis-identified as Leo Rosario at John F. Kennedy International Airport in New York and arrested. Even though he did not match the physical description of Rosario, the erroneously-cataloged fingerprints were considered to be more reliable.

Shirley McKie

Shirley McKie was a police detective in 1997 when she was accused of leaving her thumb print inside a house in Kilmarnock, Scotland where Marion Ross had been murdered. Although McKie denied having been inside the house, she was arrested in a dawn raid the following year and charged with perjury. The only evidence the prosecution had was this thumb print allegedly found at the murder scene. Two American experts testified on her behalf at her trial in May 1999 and she was found not guilty. The Scottish Criminal Record Office (SCRO) would not admit any error, although Scottish first minister Jack McConnell later said it had been an "honest mistake".

On February 7, 2006, McKie was awarded £750,000 in compensation from the Scottish Executive and the Scottish Criminal Record Office. Controversy continued to surround the McKie case and the Fingerprint Inquiry into the affair finished taking evidence in November 2009 and is awaiting publication of the final report.

Stephan Cowans

Stephan Cowans was convicted of attempted murder in 1997 after he was accused of shooting a police officer whilst fleeing a robbery in Roxbury, Massachusetts. He was implicated in the crime by the testimony of two witnesses, one of whom was the victim. There was also a fingerprint on a glass mug from which the assailant had drunk some water and experts testified that the fingerprint belonged to Cowans. He was found guilty and sent to prison for 35 years. Whilst in prison, Cowans earned money cleaning up biohazards until he

could afford to have the evidence against him tested for DNA. The DNA did not match his and he was released. He had already served six years in prison when he was released on January 23, 2004. Cowans died on October 25, 2007.

Craig D. Harvey

In April 1993, in the New York State Police Troop C scandal, Craig D. Harvey, a New York State Police trooper was charged with fabricating evidence. Harvey admitted he and another trooper lifted fingerprints from items the suspect, John Spencer, touched while in Troop C headquarters during booking. He attached the fingerprints to evidence cards and later claimed that he had pulled the fingerprints from the scene of the murder. The forged evidence was presented during John Spencer's trial and his subsequent conviction resulted in a term of 50 years to life in prison at his sentencing. Three state troopers were found guilty of fabricating fingerprint evidence and served prison sentences.

Privacy issues

Fingerprinting of children

Further information: Biometrics in schools

Various schools have implemented fingerprint locks or made a record of children's fingerprints. In the United Kingdom there have been fingerprint locks in Holland Park School in London and children's fingerprints are stored on databases. There have also been instances in Belgium, at the école Marie-José in Liège, in France and in Italy. The non-governmental organization (NGO) Privacy International in 2002 made the cautionary announcement that tens of thousands of UK school children were being fingerprinted by schools, often without the knowledge or consent of their parents. That same year, the supplier Micro Librarian Systems, which uses a technology similar to that used in US prisons and the German military, estimated that 350 schools throughout Britain were using such systems to replace library cards. By 2007, it was estimated that 3,500 schools were using such systems. Under the United Kingdom Data Protection Act, schools in the UK do not have to ask parental consent to allow such practices to take place. Parents opposed to fingerprinting may only bring individual complaints against schools. In response to a complaint which they are continuing to pursue, in 2010 the European Commission expressed 'significant concerns' over the proportionality and necessity of the practice and the lack of judicial redress, indicating that the practice may break the European Union data protection directive.

In Belgium, the practice of taking fingerprints from children gave rise to a question in Parliament on February 6, 2007 by Michel de La Motte (Humanist Democratic Centre) to the Education Minister Marie Arena, who replied that it was legal provided that the school did not use them for external purposes, or to survey the private life of children. At Angers in France, Carqueiranne College in the Var won the Big Brother Award for 2005 and the Commission nationale de informatique et des libertés (CNIL), the official organisation in charge of the protection of privacy in France, declared the measures it had introduced "disproportionate."

In March 2007, the British government was considering fingerprinting all children aged 11 to 15 and adding the prints to a government database as part of a new passport and ID card scheme and disallowing opposition for privacy concerns. All fingerprints taken would be cross-checked against prints from 900,000 unsolved crimes. Shadow Home secretary David Davis called the plan "sinister" An Early Day Motion which called on the UK Government to conduct a full and open consultation with stakeholders about the use of biometrics in schools, secured the support of 85 Members of Parliament (Early Day Motion 686). Following the establishment in the United Kingdom of a Conservative and Liberal Democratic coalition government in May 2010, the ID card scheme was scrapped.

Serious concerns about the security implications of using conventional biometric templates in schools have been raised by a number of leading IT security experts, one of whom has voiced the opinion that "it is absolutely premature to begin using 'conventional biometrics' in schools" .The vendors of biometric systems claim that their products bring benefits to schools such as improved reading skills, decreased wait times in lunch lines and increased revenues They do not cite independent research to support this view. One education specialist wrote in 2007: "I have not been able to find a single piece of published research which suggests that the use of biometrics in schools promotes healthy eating or improves reading skills amongst children... There is absolutely no evidence for such claims". The Ottawa Police in Canada have had to give advice to parents who fear that their children may be kidnapped to have their fingerprints taken.

Other uses

Welfare claimants

It has been alleged that taking the fingerprints of welfare recipients as identification serves as a social stigma that evokes cultural images associated with the processing of criminals.

Log-in authentication and other locks

Since 2000, electronic fingerprint readers have been introduced for security applications such as log-in authentication for the identification of computer users. However, some less sophisticated devices have been discovered to be vulnerable to quite simple methods of deception, such as fake fingerprints cast in gels. In 2006, fingerprint sensors gained popularity in the notebook PC market. Built-in sensors in ThinkPads, VAIO, HP Pavilion laptops, and others also double as motion detectors for document scrolling, like the scroll wheel.

Electronic registration and library access

Fingerprints and, to a lesser extent, iris scans can be used to validate electronic registration, cashless catering, and library access. By 2007, this practice was particularly widespread in UK schools, and it was also starting to be adopted in some states in the US.

Absence of fingerprints

A very rare medical condition, adermatoglyphia, is characterized by the absence of fingerprints. Affected persons have completely smooth fingertips, palms, toes and soles, but no other medical signs or symptoms. A 2011 study indicated that adermatoglyphia is caused by the improper expression of the protein SMARCAD1. The condition has been called immigration delay disease by the researchers describing it, because the congenital lack of fingerprints causes delays when affected persons attempt to prove their identity while traveling. Only four families with this condition have been described as of 2011.

People with Naegeli–Franceschetti–Jadassohn syndrome and dermatopathia pigmentosa reticularis, which are both forms of ectodermal dysplasia, also have no fingerprints. Both of these rare genetic syndromes produce other signs and symptoms as well, such as thin, brittle hair.

The anti-cancer medication capecitabine may cause the loss of fingerprints. Swelling of the fingers, such as that caused by bee stings, will in some cases cause the temporary disappearance of fingerprints, though they will return when the swelling recedes.

Fingerprints in other species

Some other animals have evolved their own unique prints, especially those whose lifestyle involves climbing or grasping wet objects; these include many primates, such as gorillas and chimpanzees, Australian koalas and aquatic mammal species such as the North American fisher. According to one study, even with an electron microscope, it can be quite difficult to distinguish between the fingerprints of a koala and a human.

Fingerprints in fiction

Mark Twain

Mark Twain's memoir Life on the Mississippi (1883), notable mainly for its account of the author's time on the river, also recounts parts of his later life, and includes tall tales and stories allegedly told to him. Among them is an involved, melodramatic account of a murder in which the killer is identified by a thumbprint. Twain's novel Pudd'nhead Wilson, published in 1893, includes a courtroom drama that turns on fingerprint identification.

Crime fiction

The use of fingerprints in crime fiction has, of course, kept pace with its use in real-life detection. Sir Arthur Conan Doyle wrote a short story about his celebrated sleuth Sherlock Holmes which features a fingerprint: The Norwood Builder is a 1903 Sherlock Holmes short story set in 1894 and involves the discovery of a bloody fingerprint which helps Holmes to expose the real criminal and free his client.

The British detective writer R. Austin Freeman's first Thorndyke novel The Red Thumb-Mark was published in 1907 and features a bloody fingerprint left on a piece of paper together with a parcel of diamonds inside a safe-box. These become the center of a medico-legal investigation led by Dr Thorndyke, who defends the accused whose fingerprint matches that on the paper, after the diamonds are stolen.

Movies

The movie Men In Black, a popular 1997 science fiction thriller, required Agent J, played by Will Smith, to remove his ten fingerprints by putting his hands on a metal ball, an action deemed necessary by the MIB agency to remove the identity of its agents. And in a 2009 science fiction movie starring Paul Giamatti, Cold Souls, a mule who is paid to smuggle souls across borders, wears latex fingerprints to frustrate airport security terminals. She can change her identity by changing her wig, and switching latex fingerprints from the privacy of a restroom, always storing extra fingerprints in a ziploc bag, so she can always assume an alias that is suitable to her undertaking.

Other reliable identifiers

Other forms of biometric identification utilizing a physical attribute that is unique to every human include iris recognition, the use of dental records in forensic dentistry, the tongue and DNA profiling, also known as genetic fingerprinting.

Fingerprint mutilation

There are several documented cases of people deliberately mutilating their fingerprints in an effort to avoid being identified from marks left on the surfaces they touch. Methods used have included burning the fingertips with acid, which John Dillinger tried and failed; prints taken during a previous arrest and upon death still exhibited almost complete relation to one another, and surgical alteration.

TECHNICAL INTRODUCTION TO GSM MODEM TECHNOLOGY

FACTS AND APPLICATIONS OF GSM/GPRS MODEM

The GSM/GPRS Modem comes with a serial interface through which the modem can be controlled using AT command interface. An antenna and a power adapter are provided.
The basic segregation of working of the modem is as under:
• Voice calls
• SMS
• GSM Data calls
• GPRS

Voice calls: Voice calls are not an application area to be targeted. In future if interfaces like a microphone and speaker are provided for some applications then this can be considered.

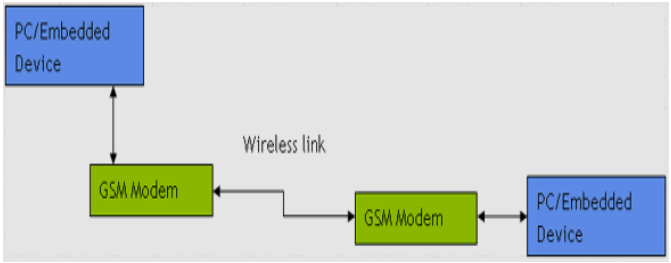
SMS: SMS is an area where the modem can be used to provide features like:
• Pre-stored SMS transmission
• These SMS can be transmitted on certain trigger events in an automation system
• SMS can also be used in areas where small text information has to be sent. The transmitter can be an automation system or machines like vending machines, collection machines or applications like positioning systems where the navigator keeps on sending SMS at particular time intervals
• SMS can be a solution where GSM data call or GPRS services are not available

GSM Data Calls: Data calls can be made using this modem. Data calls can be made to a normal PSTN modem/phone line also (even received). Data calls are basically made to send/receive data streams between two units either PC's or embedded devices. The advantage of Data calls over SMS is that both parties are capable of sending/receiving data through their terminals.

Some points to be remembered in case of data calls:
• The data call service doesn't come with a normal SIM which is purchased but has to be requested with the service provider (say Airtel).
• Upon activation of data/fax service you are provided with two separate numbers i.e. the Data call number and the Fax service number.
• Data calls are established using Circuit Switched data connections.
• Right now the speed at which data can be transmitted is 9.6 kbps.
• The modem supports speeds up to 14.4 kbps but the provider give a maximum data rate of 9.6 kbps during GSM data call.
• Technologies like HSCSD (high Speed Circuit Switched Data) will improve drastically the data rates, but still in pipeline.

Applications And Facts About GSM Data Calls:

• Devices that have communication on serial port either on PC or in the embedded environment
• Devices that want to communicate with a remote server for data transfer
• This capability of data transfer can help in reducing processing requirements of the device
• The basic aim is to provide a wireless solution keeping the existing firmware intact
• The clients firmware continues to work without any modifications (no changes in the existing software required)
• GSM data calls can be a good solution where data has to be transmitted from a hand-held device to a central server
• The interface on two sides can be between PC's as well as embedded devices



• Calls can be established by the terminals at either side to start data calls
• The Modem remains transparent during data transfer after the call is established.
• Call establishment utility to be provided in case PC terminals
• Call establishment to be automated in case of embedded terminals. GSM converter can be an option where intelligence of establishing calls has to be put in case of embedded devices. Concept of GSM converter is discussed later in this document

Dial-Up Networks Using GSM Data Calls: Dial up networking is a utility available with Windows through a person can dial the Data call number of this modem from any PC and share the file system on either PC's. This can be a good utility where both terminals are PC based. Sharing the file system remotely enables monitoring of devices remotely. Thus the modem can act as a piece of device which acts as a spy in the system. Can be a good debugging utility wherein a person can configure/monitor a remote PC based system and even rectify it. Some companies do sell their products with a GSM modem inside it just for this handy feature which allows them to configure the machines sitting anywhere in the world. Since the connection can have upper layer protocols like TCP/IP in this connection it becomes more reliable and useful.

GSM Converter: GSM converter will be an add-on device to be attached between a terminal which wants data transfer and the GSM modem. This GSM converter will take care of call establishment where the embedded device cannot make a call. The converter will remain transparent through-out the call once call is established. The GSM converter will be a very small piece of hardware possibly embedded inside the cable itself.

GPRS: This modem can be used to make a GPRS connection. Upon connection the modem can be used for internet connectivity of devices.

Key-Points in GPRS:

• The PC/Embedded device dials the Service Provider (say Airtel)
• Data is routed through the ISP (Internet Service Provider)
• GPRS is basically Packet Oriented service
• Protocols like TCP/IP are inherent characteristics in GPRS
• One has to talk in terms of IP addresses here not phone numbers
• The implementation is more useful where PC's want to communicate over GPRS
• Although data transfer is done from embedded devices too but with reduced features
• Since you are charged either on monthly flat rates or amount of data transfer taking place GPRS is any day a cheaper option as compared to GSM data call. But GPRS services are not available everywhere.
• The data rate rates in GPRS can go up to 40 kbps

Application areas in GPRS using this Modem:

• Applications where mobile devices want to upload data to a central server
• Monitoring devices that are continuously logged on to the server. Since you are charged for the amount of data transfer hence a continuous connection can be maintained.
• Virtual private networks
• Radius servers

ADVANTAGES OF SHORT MESSAGE SERVICE:

SMS is a great success all over the world. SMS messaging is one of the most important revenues of the wireless carriers. The number of messages exchanged every day is very enormous. Some of the reasons behind the popularity of the SMS are described below.

SMS messages can be sent and read at any time:

Nowadays most of the persons have a mobile phone and carries it most of the time. With a mobile phone, we can send and read messages at any time and at any place be it at the home, bus, office etc.

SMS messages can be sent to an offline mobile phone:

Unlike a phone call we can send the message to our friend when he / she has switched of the mobile phone or he /she is in the place where the wireless signal is temporarily unavailable. The SMS system of the mobile network operator will store the message and later send it to our friend.

SMS messages are less disturbing:

Unlike a phone call, we need not read or reply an SMS message immediately. Besides reading and writing the messages do not make any noise. We need not attend the messages urgently as we do in case of an urgent phone call.

SMS messages can be exchanged over different wireless carriers:

SMS technology is a very mature technology. Not only can we exchange the messages with the mobile users of same wireless carriers but also with the mobile users of different wireless carriers. So the 100% GSM phones support **Short Message Service**.

OTHER MERITS OF SHORT MESSAGE SERVICE:

- Building the wireless applications on the top of SMS technology can maximize the potential user base.
- SMS messages are capable of carrying the binary data besides the text. They can be used to transfer the ring tones, pictures, operator logos, wallpapers, animations, VC cards etc.
- Thirdly SMS supports **reverse billing** which enables payment to be made conveniently.

APPLICATIONS OF SHORT MESSAGE SERVICES:

There are many different kinds of SMS applications on the market today and many others can be developed. Applications in which the SMS messaging can be utilized are Virtually unlimited. Some of the applications are described below.

Person-to-Person Text Messaging:

Person to person text messaging is the most commonly used SMS application. Here, a person types a text message to his friend using the keypad of his mobile phone and then inputs the mobile phone number of the recipient and clicks the **Send** option on the screen to send the message out. When the recipient mobile phone receives the sent text message

It will notify the user by giving out a sound or a vibration. The recipient can then read and respond either immediately or at any time later.

Provision of information:

It is another popular application of the SMS technology. Many content providers make use of the SMS text messages to send the information such as news, weather report and financial data to their subscribers. Many of these information services are not free.

Downloading:

SMS can be used as a transport medium of wireless downloads since it carries binary data. Objects such as pictures, wallpapers, and logos can be encoded in one or more SMS messages depending upon the object's size. Like information services wireless download services are also not free.

Alerts and Notifications

SMS is a very suitable technology for delivering alerts and notifications of important events. This is because of two reasons:

- A mobile phone is a device that is carried by its owner most of the time. Whenever an SMS text message is received, the mobile phone will notify you by giving out a sound or by vibrating. You can check what the SMS text message contains immediately.
- SMS technology allows the "push" of information. This is different from the "pull" model where a device has to poll the server regularly in order to check whether there is any new information. The "pull" model is less suitable for alert and notification applications, since it wastes bandwidth and increases server load.

Email, Fax and Voice Message Notifications

In an email notification system, a server sends a text message to the user's mobile phone whenever an email arrives at the inbox. The

SMS text message can include the sender's email address, the subject and the first few lines of the email body. An email notification system may allow the user to customize various filters so that an SMS alert is sent only if the email message contains certain keywords or if the email sender is an important person. The use cases for fax or voice message are similar.

HOW TO SEND MESSAGES TO THE SYSTEM?

The SMS specification has defined a way for a computer to send and receive messages through a mobile phone or a GSM modem. A GSM modem is a wireless modem that works with GSM wireless networks. This wireless modem transmits the data through the wireless network.

To send the SMS messages, first a valid SIM card is placed from a wireless carrier into a mobile phone or a GSM modem, which is then connected to the computer. There are several ways of making interaction between a computer and a mobile phone. These are through the **USB cable, Serial cable, Blue Tooth link or an infrared link**.

But the actual way to use depends upon the capability of the GSM modem or mobile phone. If a mobile phone does not support Blue Tooth, it cannot get connected to the computer through the Blue Tooth link.

After connecting the mobile or GSM modem, we can control the system by sending the instructions to it that is in the form of messages.

The instructions that we give and the messages we receive is fully controlled by the software that we are using to control the system.

We should write a source code for connecting the mobile to the system and sending and receiving commands to and fro between the GSM modem and the system. This source code can be written in **C, C++,JAVA,VISUAL BASIC,DELPHI** or any programming languages.

HOW TO RECEIVE MESSAGES FROM SYSTEM?

There are three ways to receive the messages using the Personal Computers.

- Connect a mobile phone or a GSM modem to the computer. Then use the computer commands to get the received messages from the mobile phones or GSM modem.

- Get access to the SMS Center (SMSC) or SMS gateway of a wireless carrier. Any SMS message received will be forwarded to the computer using a protocol or interface supported by the SMSC or SMS gateway.

- Get access to the SMS gateway of an SMS service provider. Any SMS message received will be forwarded to the computer or PC using the protocol or interface supported by the SMS gateway.

Receiving the messages from the system using the first way has a major advantage over the other two ways. Wireless carriers do not charge any fee for receiving the incoming messages with their SIM cards. Nevertheless the disadvantage is that a mobile phone or a GSM modem cannot handle a large amount of SMS traffic. One way to overcome is to balance the traffic using a pool of mobile phones or GSM modems. But this is not a big disadvantage for my project.

ADVANTAGE:

- High reliable.
- Unique.
- Processing speed is fast.
- Easy to use & user friendly.
- Highly secured than other security systems.

APPLICATION:

- Cars.
- Motorcycles.
- Transport vehicles
- Home security systems
- Lockers
- ATM’s

Working and block diagram:-

Human identification is field very significant and which has undergone rap id changes with time. An important and very reliable human identification method is fingerprint identification. Fingerprint of every person is unique. So this helps in identifying a person or in improving security of a system.

In this paper we use a fingerprint module to read once identity to start the vehicle. For this we use a microcontroller to enable the ignition system if the matching between scanned data and the already existing data is correct. Comparison is done inside the finger print module itself and its output is given to microcontroller. Result is displayed in a LCD display whether the user is authorised or not .If the Scanned data is not matched message will be send to authorised user through GSM module.

In this project embedded system plays major role. It consist of Level converter, GSM, Finger Print sensor, Driver, Display and Power supply. Level converter is used to convert signal CMOSS to TTL and TTL to CMOSS. Fingerprint sensor is identifying the authorised user or not. It is connected to the Embedded system through Level converter. Vehicle connected to Embedded system through driver. Power supply is used to supply the system.

CONCLUSION

Thus fingerprint identification enhances the security of a vehicle and makes it possible only for some selected people to start the vehicle. Thus by implementing this relatively cheap and easily available system on a vehicle one can ensure much greater security and exclusivity than that offered by a conventional lock and key.

BIBLIOGRAPHY:

Integrated Electronics by Millman & halkias

Hitch C PIC manual

PIC reference by Myke Predko

Power supply design

Electrical technology by theraja

Let us c by kanetkar

Embedded c by Kenneth.J.Ayala

WEBSITES:

www.alldatasheet.com

www.atmel.com

www.microchip.com

www.nationalsemiconductor.com

www.google.com