**FACE RECOGNITION BASED ATM SECURITY**

**USING ARDUINO**

**INTRODUCTION**

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearences. Using the proper PIN gains access, the successful transactions can occur, but the user of the PIN is not verified. When ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. This paper describes how face recognition technology can help to the real world ATM machines.

The first step is the capturing of a face image. This would normally be done using a still or video camera. The face image is passed to the recognition software for recognition (identification or verification). This would normally involve a number of steps such as normalizing the face image and then creating a ‘template’ of ‘print’ to be compared to those in the database. The match can either be a true match which would lead to investigative action or it might be a ‘false positive’ which means the recognition algorithm made a mistake and the alarm would be cancelled. Each element of the system can be located at different locations within a network, making it easy for a single operator to respond to a variety of systems.

An Automatic Teller Machine (ATM) is a computerized machine that is used to withdraw cash from a customer’s respective bank account. As financial users prefer ATM for cash withdrawals, cash deposits and many other transactions, the banks are focusing a lot over the security of ATMs. Hence ATM should be protected properly from the criminal activities or from any unwanted things. Due to rapid development in science and technology, upcoming innovations are being built-up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, various financial institutions like banks and applications like ATM are still subjected to thefts and frauds. The existing ATM model uses a card and a PIN which gives rise to increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats. Then another major problem is hacking of PIN. There are other fraudulent attacks like eavesdropping, spoofing, brute force attacks, blackmailing the user. In the worst case there can also be ATM machine Robbery. To overcome these problems, the project ’ATM Security system based on Face recognition, PIN and OTP’ consists of conventional features ie is Personal Identification Number (PIN) along with additional features like face recognition and one-time password (OTP) is used. Database holds information about a user’s ac- count details, images of his/her face and a mobile number which will improve security to a large extent. First, the user will come to the ATM machine and a live image is captured through the Web Camera interfaced with System defining as the ATM system, which is compared with the images stored in the database. If the face is recognized, then the user is notified to type the PIN. If the PIN matches, an OTP will be sent to the corresponding registered mobile number. If the user correctly enters the OTP, the transaction can proceed. Therefore, the combination of face recognition algorithm, PIN and an OTP drastically reduces the chances of fraud. In order to obtain better accuracy deep learning based linear discriminate classification method is utilized. And executed the same in OS.

**ABSTRACT**

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. Proposed paper uses face recognition technique for verification in ATM system. For face recognition, there are two types of comparisons. The first is verification, this is where the system compares the given individual with who that individual says they are and gives a yes or no decision. The next one is identification this is where the system compares the given individual to all the other individuals in the database and gives a ranked list of matches. Face recognition technology analyzes the unique shape, pattern and positioning of the facial features. Face recognition is very complex technology and is largely software based. This Biometric Methodology establishes the analysis framework with PCA algorithms for each type of biometric device. Face recognition starts with a picture, attempting to find a person in the image. This can be accomplished using several methods including movement, skin tones, or blurred human shapes.

Programmed acknowledgement of people has been a testing errand since quite a while and no such adaptable and powerful framework has been planned so far that could give total human acknowledgement access and security to critical data and physical assets among the different acknowledgement strategies have advanced essentially in the most recent decade and develop to a promising region to distinguish people be that as it may, the dependability of face acknowledgement strategies still require testing assignments to be performed by the exploration network to build up a profoundly Vigorous framework by defeating conceivable facial appearance variety .In this paper, we present a biometric based framework known as face acknowledgement calculation consequently hand off will be on ,and engine pivots shows as entry way shutting. This application is process in ATM security framework to improve the verification strategies to improve the innovation.

**OBJECTIVE**

The objective of this study is as follow: -

* To provide a platform that will allow the bankers to collect customers’ face recognition data.
* To provide a platform that will allow the bankers to collect customers’ phone number and store them in a centralized database.
* To build a system that will forward 4-digit number to the customers’ mobile phone when the face detection matches.
* To provide a platform that allows the customer to run his transaction after the system accepts the code generated.
* To create a platform that will be able to analyze biometric data in the global image analysis.
* To propose the authentication system on the existing ATM process for withdrawal after the entry of a correct pin.
* To propose second level authentication system in a scenario where customer specified withdrawal limit.
* To introduce the confirmation framework on the current ATM measure for withdrawal after the passage of a right pin.
* To introduce a second level verification framework in a situation where the client indicated withdrawal limit.

**Security:**

The main objective of face detecting ATM system is to protect security.

**Welfare Claimants:**

It has been alleged that taking the face detecting 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:**

 Electronic face detecting readers have been introduced for security applicationssuch 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 face detectings.

**Electronic registration:**

 face detectings and to a lesser extent,it is used to validate the electronic registration.

**Functional Requirements:**

**Withdrawal -**The user selects withdraw from the menu and withdraws cash  from the  ATM.

**Deposit -**The user selects deposit option from the menu and deposits cash or cheques into the ATM.

**Print transaction -**ATM prints a record after a transaction.

**Exits -**user completes session with ATM and retrievescard.

**Non - Functional Requirements:**

**Safety Requirement - S**ystem use shall not cause any harm to humanusers.

**Security Requirements -**System will use secured database.Normal userscan just read information but they can't edit ormodify anything except their personal and someother information system will have differenttypes of users and every user has accesscontrains.

**Performance Requirement**- The system shall accomidate high number ofusers without any fault.

**Reliabilit**- The application should be relaible and itshould generate all updated information incorrect order

**Availability**- Application will be available and working properly for all the time it should be available inseveral languages

**LITERATURE REVIEW**

* Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years. A lot of criminals tamper with the ATM terminal and steal customers’ card details by illegal means. Once users’ bank card is lost and the password is stolen, the users’ account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects .
* The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem since a person’s biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card. Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioral characteristic. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity.
* Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.
* Mohsin Karovaliya in paper proposes Eigenface based method for the face recognition. This system analyzes the algorithms used in the previous systems. PCA based algorithm is more reliable, very fast and the storage space takes is very less. The main drawback this method is that it can be manipulated by using photos of users. This method can be improved by using 3D face masks but the cost of making 3D masks is very high.
* The paper suggests a vibration sensor which senses vibrations produced from ATM machine whenever robbery occurs. This system processes realtime data collected by the vibration sensor using an ARM controller-based embedded system. The buzzer will emit a beep sound once the vibration is detected. The ATM door is closed with a DC motor. There are also some additional security measures in place. This will deter theft and make it possible to arrest the suspect. Two software programs are used to execute the software, the first of which is Keil Vision 3.0. The Flash magic simulator is the second. Keil Vision Debugger correctly simulates on-chip peripherals. This device aids in rapid reaction and minimization of failure by detecting the ATM machine at real-time when it has been stolen can be identified by GSM technology.
* In paper, the finger print recognition is done with curvelet transform by finding the Euclidean distance between the two corresponding finger codes. The test finger code is compared with the entire finger codes in the database. An OTP will be sent to the matching registered mobile number if it matches. The built-in MATLAB feature ‘imread' is used for preprocessing. The histogram equalization approach improves an image's global contrast by shifting the intensity distribution on a histogram marginally. This helps lowcontrast areas to achieve more contrast without affecting the overall contrast. This is achieved by histogram equalization, which essentially spreads out the most common strength values. Curvelet transform and FFT can also be used for function extraction.
* The ATM security is enhanced by adding GSM module to generate OTP in paper. Where there is a network issue with GSM technologies, this system uses Bluetooth to link to an ATM, which produces an OTP relation from the user's cell phone. Since no special subscription to an SMS service provider is needed, GSM modems can be a fast and easy way to get started with SMS. A GSM modem can also be a regular GSM phone with the required cable and software. A GSM modem may also be a regular GSM phone with the required cable and software driver to connect to a serial port or USB port.
* Financial institutions have registered major loses till today due to users being exposed of their credit and debit card information. For secure PIN authentication, in this paper, we propose Secure-PINAuthentication-as-a-Service (SEPIA), a secure obfuscated PIN authentication protocol for ATM and other point-of-service terminals using cloud-connected personal mobile and wearable devices. It protects the user from intermediate transaction attacks. A SEPIA user utilizes a mobile device for scanning or QR code on the terminal screen to prove co-location to the cloud-based server and obtain a secure PIN template for point-of-service authentication.
* Features like face recognition and one time password are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. This eliminates the chances of fraud due to theft and duplicity of the ATM cards. Moreover, the randomly generated OTP frees the user from remembering PINs as it itself acts as a PIN.
* ATM are widely used nowadays by people. But It’s hard if we forget the PIN number or it may get damaged and users can have a situation where they can’t get access to their money. In this the use of biometrics for authentication instead of PIN and ATM card is encouraged. Here, The Face ID and Fingerprint are preferred to high priority. The fingerprint is preferred to high priority. The fingerprint of the user is identified and face image is verified, and the appropriate user is given authentication. For the prototype of the system, Raspberry pi microcontroller is used.
* Faces are represented by labeled graphs, based on a Gabor wavelet transform.Image graphs of new faces are extracted by an elastic graph matching process and can be compared by a simple similarity function. Phase information is used for accurate node positioning. Object-adapted graphs are used to handle large rotations in depth.
* ATM with a currency dispenser includes a contactless card reader that can read data from an RFID tag of a customer’s ATM card. The contactless card reader can also be used in conjunction with a magnetic stripe card reader. It is able to prevent the missing of the ATM card and dispensed money by the customer inside the ATM centre after the transaction.
* An automatic teller machine security model that would combine a physical access card, a PIN, and electronic facial recognition having access only to actual owner of the card .Denis et. al. explores the difficulties in Blockchain IoT applications, and outlines the huge work in order to analyze how Blockchain could be utilized in real money coordination. The author in has examined the different error codes thrown by various ATM machines produced by different manufacturers and proposed a common code for very similar malfunctions made by the machine.

**EXISTING SYSTEM**

In modern days, Everyone used to do banking like storing cash and withdrawing cash. The clients will be in line to extract cash from the bank. The clients felt like biding one’s time to withdraw money. That bank proposes an ATM (Automated teller machine) to aid the client extract cash quickly. In such an ATM, they propose CARDS (Visa, Credit, master, Debit) to the client to extract money through their usage. Major merit is fast money provided by the ATM. The customers feel joyful and they shall not throw away time to take out money being in queue. Still it has a main limitation like, physical keys and smart cards, may be theft, misplaced, duplicated, or forgotten; passwords may get distributed, unremembered, hacked or seen by some third party. Banks needed a good mechanism to manage protection for the clients to make the transaction in the banks.

In present days the ATM holds only one thing (i.e. PIN) to secure the money saved in the bank and if we are not considering the physical attacks.

* User enters the card to machine.
* Card Reader reads the information on the magnetic strip on the card and sends the information to the bank server. If the card information is valid according to the bank, the ATM will ask for PIN.
* User will enter PIN to the ATM machine.
* If PIN entered by User is correct according to server, User will be allowed further to access for transactions.
* This is process will only be applicable for one time, i.e. if user want to withdraw more money than he/she have to repeat the process again.

But there are problems and vulnerabilities in the present

system.

* It is possible that the machine is tempered and read wrong information as correct information.
* It is also possible that the magnetic strips hold legitimate information but that card is duplicated.
* PIN can be hacked by any means like shoulder surfing, mutual friends, family friends etc.
* After PIN is correct there is no one who can catch attacker to steal money from bank. It is just like stealing from cupboard. Current ATM system is not the safest system for the most important asset of human being i.e. Money. There is a need of some new system which is easy to adapt and more secure.

**PRESENT ATM**

A computerized technology that establishes the role of being a monetary medium between the clients and the bank to maintain the functionality of transactions without the presence of a third party. Some charge cards, be that as it may, may experience more difficulty. ATMs are highly feasible because it allows the clients to perform any required transaction without having the obligation to go to the bank.

The PIN stands for Personal Identification Number. It is a combination of four numbers, each one ranging from 0 to 9 amounts to a decade of PINs possible, which is preferably set by the clients. This PIN remains universal throughout the longevity of the bank account until unless it is not changed by the client. Since it is modicum in size, it can be swiftly memorized. The hacker has every technological tool at their disposal to guess the accurate PIN. When the client enters the PIN on the ATM screen then it is cross-examined from the database of the bank organizations.

The present ATM works in such a way that the person first enters the ATM. He/she inserts his/her ATM card into the machine. Then, they enter the ATM PIN for verifying that they are the owner of the ATM Card. After the verification, they select the type of Accounts from which they want to withdraw money. If they have sufficient balance in their account, the ATM dispenses the amount and informed them via a Text Message / Email about the transaction successful and remaining balance present in the amount.

**LIMITATIONS**

* If problem with credit card you cannot withdraw your money.



* If someone watches or hacks an ATM machine your details may be taken if you forget your PIN number you cannot use the card. 
* Cannot be provided in rural areas: In a country like India, where banks are having large number of rural and non-computerized branches, ATM services cannot be provided. 
* Limitation of cash withdrawals: Again there is a limitation of cash withdrawals from ATM. For example, many banks do not permit withdrawal of more than 25,000 at a time. 
* Cash deposit facility is not safe: Similarly cash deposit facility is restricted and not safe as dropping of envelope and ATM is not advisable. Possibility of misusing ATM card: ATM card, if misplaced, lost or stolen, may be misused. There are number of such reported incidences now a day. 
* Loss of personal touch with the Banks: Last but not the least; customers lose personal touch with their bankers.

**PROPOSED SYSTEM**

In this project we will rectify the above problems and it will be overcome by providing a high security to the users while doing a transaction in the ATM. To provide a secured transaction the pinhole camera which we had already fixed in the ATM machine will take a snap of the person who is going to credit the amount from the ATM. Then the captured image of the person will be compared with the account holder image in the respective bank database. If the user image gets matched with the anyone of the image in the database means then automatically it will allow the user to perform any operations like withdraw or transaction in the ATM. Whereas the other possibility will be, if the user image does not gets matched with any of the image from the account holders profile in the bank database within a fraction of second a message will be send as a link to the account holder registered mobile number. If the user (account holder) clicks the link it will show the snap of the person who is currently using their ATM card to withdraw money from the ATM. And it will also enable three options to the user to choose any one of the option. The three options are it’s me, Accept and Decline.

**Advantages of Face detecting over other Biometric Methods**

*  It is unique for every individual.
*  Easy to install compared with other biometrics.
*  Robust and easy to use.
*  Low maintenance cost.
*  Since is already available in the banker’s database, so no extra cost for database management.

**APPLICATIONS OF BIOMETRIC SYSTEM :**

* The biometrics can be used mainly used for Security purposes such as Counterterrorism, Access control, comparing surveillance images to know terrorist. 
* It can be used in schools to verify the identity of individuals picking up children from schools. 
* It is also helpful for increasing the residential Security as it will alert the homeowners of approaching unknown persons. 
* One of the applications of biometrics is in Voter verification, where eligible politicians are required to verify their identity during a voting process this is intended to stop voting where the vote may not go as expected. 
* And one of the most vital applications of biometrics is in the field of the Banking system to verify the authorized person.

**ADVANTAGES OF PROPOSED SYSTEM :**

* It will give foolproof authentication.



* It is very effective as compared to other methods. 
* Biometric tokens are the safest means of preventing ATM frauds.
* The one-time password sends by GSM modem to the user changes every time so it provides good security. 
* People are forced to remember many passwords. But biometric technology does not require the use of any Password or PIN.
* In some application, biometrics can replace or reestablish the existing technology.
* Biometric systems have less error rate and it is convenient to use.
* It is very easy to implement and use.
* It is very efficient as compared to other methods.
* Moreover, it does not depend on any kind of technique that uses skin tone as one of its feature to be used for identification.
* It provide more security.
* No backup plan suggested to overcome the failure of face detection or OTP system.
* Biometric tokens are the safest means of preventing ATM frauds.
* In some application biometrics can replace or supplement the existing technology, in others, it is the only viable approach.

**BLOCK DIAGRAM**

**RFID Reader**

**Mail**

**Buzzer**

**RFID Tag**

**Face Recognition System**

**Arduino UNO**

**Relay**

**DC Motor**

**PC**

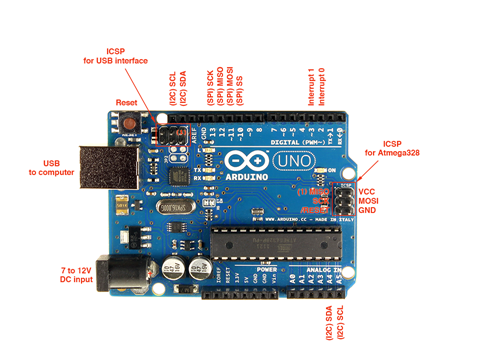
**HARDWARE MODULES**

* Arduino UNO
* RFID Reader & Tag
* Camera
* Relay
* DC Motor
* Buzzer

**Arduino**

**Microcontroller**

A micro-controller is a small computer on a single integrated circuit containing a processor core, memory, and programmable input/ output peripherals The important part for us is that amicro-controller contains the processor (which all computers have) and memory, and some input/output pins that you can control. (often called GPIO - General Purpose Input Output Pins).



We will be using the Arduino Uno board. This combines a micro-controller along with all of the extras to make it easy for you to build and debug your projects. The Uno is a microcontroller board based on the [ATmega328P.](http://www.atmel.com/images/Atmel-8271-8-bit-AVR-Microcontroller-ATmega48A-48PA-88A-88PA-168A-168PA-328-328P_datasheet_Complete.pdf)It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.. You can tinker with your UNO without worrying too much about doing something wrong, worst case scenario you can replace the chip for a few dollars and start over again.

"Uno" means one in Italian and was chosen to mark the release of Arduino Software (IDE) 1.0. The Uno board and version 1.0 of Arduino Software (IDE) were the reference versions of Arduino, now evolved to newer releases. The Uno board is the first in a series of USB Arduino boards, and the reference model for the Arduino platform; for an extensive list of current, past or outdated boards see the Arduino index of boards.

This is a relatively easy way to make circuits quickly. Breadboards are made for doing quick experiments. They are not known for keeping circuits together for a long time. When you are ready to make a project that you want to stay around for a while, you should consider an alternative method such as wire-wrapping or soldering or even making a printed circuit board (PCB). The first thing you should notice about the breadboard is all of the holes. These are broken up into 2 sets of columns and a set of rows (the rows are divided in themiddle). The columns are named a, b, c, d, e, f, g, h, i, and j (from left to right). The rows are numbered 1 - 30. (from top to bottom). The columns on the edges do not have letters or numbers. The columns on the edges are connected from top to bottom inside of the breadboard to make it easy to supply power and ground. (You can think of ground as the negative side of a battery and the power as the positive side.) For this book our power will be +5 volts. Inside of the breadboard, the holes in each row are connected up to the break in the middle of the board. For Example: a1,b1,c1,d1,e1 all have a wire inside of the breadboard to connect them. Then f1, g1, h1, i1, and j1 are all connected. but a1 is not connected to f1. This may sound confusing now, but itwill quickly come to make sense as we wire up circuits.

**Programming**

The Uno can be programmed with the Arduino Software (IDE). Select "Arduino/Genuino Uno" from the Tools > Board menu (according to the microcontroller on your board). For details, see the reference and tutorials.

The ATmega328 on the Uno comes preprogrammed with a bootloader that allows you to upload new code to it without the use of an external hardware programmer. It communicates using the original STK500 protocol (reference, C header files).

You can also bypass the bootloader and program the microcontroller through the ICSP (In-Circuit Serial Programming) header using Arduino ISP or similar; see these instructions for details. The ATmega16U2 (or 8U2 in the rev1 and rev2 boards) firmware source code is available in the Arduino repository. The ATmega16U2/8U2 is loaded with a DFU bootloader, which can be activated by:

* On Rev1 boards: connecting the solder jumper on the back of the board (near the map of Italy) and then rese ing the 8U2.
* On Rev2 or later boards: there is a resistor that pulling the 8U2/16U2 HWB line to ground, making it easier to put into DFU mode.

You can then use Atmel's FLIP software (Windows) or the DFU programmer (Mac OS X and Linux) to load a new firmware. Or you can use the ISP header with an external programmer (overwriting the DFU bootloader). See this user-contributed tutorial for more information.

**Warnings**

The Uno has a resettable polyfuse that protects your computer's USB ports from shorts and overcurrent. Although most computers provide their own internal protection, the fuse provides an extra layer of protection. If more than 500 mA is applied to the USB port, the fuse will automatically break the connection until the short or overload is removed.

**Differences with other boards**

The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter.

**Power**

The Uno board can be powered via the USB connection or with an external power supply. The power source is selected automatically. External (non-USB) power can come either from an AC-to-DC adapter (wall-wart) or battery. The adapter can be connected by plugging a 2.1mm center-positive plug into the board's power jack. Leads from a battery can be inserted in the GND and Vin pin headers of the POWER connector.

The board can operate on an external supply from 6 to 20 volts. If supplied with less than 7V, however, the 5V pin may supply less than five volts and the board may become unstable. If using more than 12V, the voltage regulator may overheat and damage the board. The recommended range is 7 to 12 volts.

* The power pins are as follows:  
  Vin. The input voltage to the Uno board when it's using an external power source (as opposed to 5 volts from the USB connection or other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin.
* 5V.This pin outputs a regulated 5V from the regulator on the board. The board can be supplied with power either from the DC power jack (7 - 12V), the USB connector (5V), or the VIN pin of the board (7-12V). Supplying voltage via the 5V or 3.3V pins bypasses the regulator, and can damage your board. We don't advise it.
* 3V3. A 3.3 volt supply generated by the on-board regulator. Maximum current draw is 50 mA.
* GND. Ground pins.
* IOREF. This pin on the Uno board provides the voltage reference with which the microcontroller operates. A properly configured shield can read the IOREF pin voltage and select the appropriate power source or enable voltage translators on the outputs to work with the 5V or 3.3V.

**Memory**

The ATmega328 has 32 KB (with 0.5 KB occupied by the bootloader). It also has 2 KB of SRAM and 1 KB of EEPROM (which can be read and written with the EEPROM library).

**Input and Output**

See the mapping between Arduino pins and ATmega328P ports. The mapping for the Atmega8, 168, and 328 is identical. Each of the 14 digital pins on the Uno can be used as an input or output, using pinMode(),digitalWrite(), and digitalRead() functions. They operate at 5 volts. Each pin can provide or receive 20 mA as recommended operating condition and has an internal pull-up resistor (disconnected by default) of 20-50k ohm. A maximum of 40mA is the value that must not be exceeded on any I/O pin to avoid permanent damage to the microcontroller.

In addition, some pins have specialized functions:

* Serial: 0 (RX) and 1 (TX). Used to receive (RX) and transmit (TX) TTL serial data. These pins are connected to the corresponding pins of the ATmega8U2 USB-to-TTL Serial chip.
* External Interrupts: 2 and 3. These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value. See the attachInterrupt() function for details.
* PWM: 3, 5, 6, 9, 10, and 11. Provide 8-bit PWM output with the analogWrite() function.
* SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). These pins support SPI communication using the SPI library.
* LED: 13. There is a built-in LED driven by digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off.
* TWI: A4 or SDA pin and A5 or SCL pin. Support TWI communication using the Wire library.

The Uno has 6 analog inputs, labeled A0 through A5, each of which provide 10 bits of resolution (i.e. 1024 different values). By default they measure from ground to 5 volts, though is it possible to change the upper end of their range using the AREF pin and the analogReference() function.

There are a couple of other pins on the board:

* AREF. Reference voltage for the analog inputs. Used with analogReference().
* Reset. Bring this line LOW to reset the microcontroller. Typically used to add a reset button to shields which block the one on the board.

**Communication**

The Uno has a number of facilities for communicating with a computer, another Uno board, or other microcontrollers. The ATmega328 provides UART TTL (5V) serial communication, which is available on digital pins 0 (RX) and 1 (TX). An ATmega16U2 on the board channels this serial communication over USB and appears as a virtual com port to software on the computer. The 16U2 firmware uses the standard USB COM drivers, and no external driver is needed.

However, on Windows, a .inf file is required. The Arduino Software (IDE) includes a serial monitor which allows simple textual data to be sent to and from the board. The RX and TX LEDs on the board will flash when data is being transmitted via the USB-to-serial chip and USB connection to the computer (but not for serial communication on pins 0 and 1. A SoftwareSerial library allows serial communication on any of the Uno's digital pins.

The ATmega328 also supports I2C (TWI) and SPI communication. The Arduino Software (IDE) includes a Wire library to simplify use of the I2C bus; see the documentation for details. For SPI communication, use the SPI library.

**Automatic (Software) Reset**

Rather than requiring a physical press of the reset button before an upload, the Uno board is designed in a way that allows it to be reset by software running on a connected computer. One of the hardware flow control lines (DTR) of the ATmega8U2/16U2 is connected to the reset line of the ATmega328 via a 100 nanofarad capacitor. When this line is asserted (taken low), the reset line drops long enough to reset the chip. The Arduino Software (IDE) uses this capability to allow you to upload code by simply pressing the upload button in the interface toolbar. This means that the bootloader can have a shorter timeout, as the lowering of DTR can be well-coordinated with the start of the upload.

This setup has other implications. When the Uno is connected to either a computer running Mac OS X or Linux, it resets each time a connection is made to it from software (via USB). For the following half-second or so, the bootloader is running on the Uno. While it is programmed to ignore malformed data (i.e. anything besides an upload of new code), it will intercept the first few bytes of data sent to the board after a connection is opened. If a sketch running on the board receives one-time configuration or other data when it first starts, make sure that the software with which it communicates waits a second after opening the connection and before sending this data.

The Uno board contains a trace that can be cut to disable the auto-reset. The pads on either side of the trace can be soldered together to re-enable it. It's labeled "RESET-EN". You may also be able to disable the auto-reset by connecting a 110 ohm resistor from 5V to the reset line; see this forum thread for details.

**Revisions**

Revision 3 of the board has the following new features:

* pinout: added SDA and SCL pins that are near to the AREF pin and two other new pins placed near to the RESET pin, the IOREF that allow the shields to adapt to the voltage provided from the board. In future, shields will be compatible with both the board that uses the AVR, which operates with 5V and with the Arduino Due that operates with 3.3V. The second one is a not connected pin, that is reserved for future purposes.
* Stronger RESET circuit.
* Atmega 16U2 replace the 8U2.

**Automatic (Software) Reset**

Rather than requiring a physical press of the reset button before an upload, the Arduino Uno is designed in a way that allows it to be reset by software running on a connected computer. One of the hardware flow control lines (DTR) of the ATmega8U2/16U2 is connected to the reset line of the ATmega328 via a 100 nanofarad capacitor. When this line is asserted (taken low), the reset line drops long enough to reset the chip. The Arduino software uses this capability to allow you to upload code by simply pressing the upload button in the Arduino environment. This means that the bootloader can have a shorter timeout, as the lowering of DTR can be well-coordinated with the start of the upload. This setup has other implications. When the Uno is connected to either a computer running Mac OS X or Linux, it resets each time a connection is made to it from software (via USB). For the following halfsecond or so, the bootloader is running on the Uno. While it is programmed to ignore malformed data (i.e. anything besides an upload of new code), it will intercept the first few bytes of data sent to the board after a connection is opened. If a sketch running on the board receives one-time configuration or other data when it first starts, make sure that the software with which it communicates waits a second after opening the connection and before sending this data. The Uno contains a trace that can be cut to disable the auto-reset. The pads on either side of the trace can be soldered together to re-enable it. It's labeled "RESET-EN". You may also be able to disable the auto-reset by connecting a 110 ohm resistor from 5V to the reset line; see this forum thread for details.

**USB Overcurrent Protection**

The Arduino Uno has a resettable polyfuse that protects your computer's USB ports from shorts and overcurrent. Although most computers provide their own internal protection, the fuse provides an extra layer of protection. If more than 500 mA is applied to the USB port, the fuse will automatically break the connection until the short or overload is removed.

**Physical Characteristics**

The maximum length and width of the Uno PCB are 2.7 and 2.1 inches respectively, with the USB connector and power jack extending beyond the former dimension. Four screw holes allow the board to be attached to a surface or case. Note that the distance between digital pins 7 and 8 is 160 mil (0.16"), not an even multiple of the 100 mil spacing of the other pins.

**SOFTWARE TIPS**

When bootloading na Atmega8 chip with Arduino 0010, there is a command (-i800) that makes bootloader delay 10 minutes. So, if you need to use bootloader, use command line instead of IDE, removing “–i800” command and adding “–F” command, or use Arduino 0007 IDE. To upload sketches Arduino 0010 works fine.

ARDUINO S3v3 NEW FEATURES

* full compatible with Shield Boards (Version 2 is the only Arduino Board not compatible with Shield Boards because of ICSP header wrong position, and tall components);
* AVcc LP filter to reduce noise level on ADC;
* auto reset feature;
* auto reset enable/disable jumper, to avoid not desired reseting;
* arduino Diecimila compatible reset pin;
* pin13 onboard led, with current limiter resistor;
* TX and RX onboard leds;
* power led with appropriate current limiter resistor (less 20mA of comsumption);
* jumper to disable serial communication and to enable RX external pull down resistor, to avoid “RX floating error”. This feature allows to use digital pin0 and pin1 as a normal pin, when serial communication is not needed;
* all similar components (diodes, transistors, leds, capacitors) has the same board orientation (to makes easier to mount with less mistakes);
* no wires between pads, more space between wires, larger wires, larger pads (better for etching, soldering and drilling, with no short circuits, soldering bridges or open wires in corrosion);
* only 3 wire bridges;
* electrolitic capacitor (in serial to TTL circuit) changed to bipolar type (to avoid inverted voltage problem when serial cable is not connected);
* All jumpers are right angle type, to allow Shield Boards use.

1. **CAMERA**

PRINCIPLE**:**

A camera records and stores photographic image in digital form. Many current models are also able to capture sound or video, in addition to still images. Capture is usually accomplished by use of a photo sensor, using a charged coupled device.

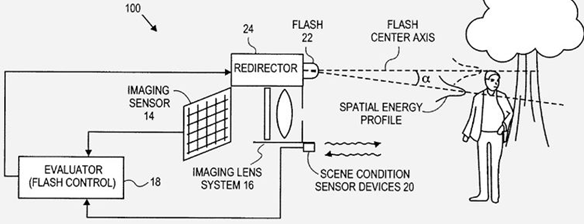
PRODUCT FEATURES:

The images are actually stored as a several pixel, for every pixel in the sensor, the brightness data, represented by a number from 0 to 4095 for a 12-bit A/D converter, along with the coordinates of the location of the pixel, are stored in a file. Although the camera can record 12 bits or 4096 steps of brightness information, almost all output devices can only display 8 bits or 256 steps per color channel. The original 12-bit (212 = 4096) input data must be converted to 8-bits (28 = 256) for output. the indicated pixel has a brightness level of 252 in the red channel, 231 in the green channel, and 217 in the blue channel. Each color's brightness can range from 0 to 255, for 256 total steps in each color channel when it is displayed on a computer monitor, or output to a desktop printer. Zero indicates pure black, and 255 indicates pure white. 256 colors each of red, green and blue may not seem like a lot, but actually it is a huge number because 256 x 256 x 256 = more then 16 million individual colors

OPERATION:

An image sensor is an electronic, photosensitive device which converts an optical image into an electronic signal. It is composed of millions of photodiodes and is used as an image receiver in digital imaging equipment. An image sensor is capable of reacting to the impact of photons, thus converting them into an electrical current that is then passed onto an analog-digital converter. The most common types of image sensors are CCD and CMOS sensors. Image sensors are mostly used in camera modules, digital cameras and other imaging devices. Some of the earliest analog sensors were video camera tubes. Currently, the most common image sensors are digital charge-coupled device (CCD) or complementary metal–oxide–semiconductor (CMOS) active pixel sensors. In a camera, a photo electronic image sensor converts the light passing through the lens into per-photodiode charges of varying sizes. These charges are then processed by the camera’s electronics and are converted into image information by the camera’s software. Applications in the dental x-ray field include intra-oral, panoramic imaging.

When the operation start at camera, an aperture opens at the front of the camera and light streams in through the lens.  There is a piece of electronic equipment that captures the incoming light rays and turns them into electrical signals. This light detector is one of two types, either a charge-coupled device (CCD) or a CMOS image sensor. In a camera, Light from the thing you are photographing zooms into the camera lens. This incoming "picture" hits the image sensor chip, which breaks it up into millions of pixels. The sensor measures the color and brightness of each pixel and stores it as a number. Your digital photograph is effectively an enormously long string of numbers describing the exact details of each pixel it contains.



1. **BUZZER:**

A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave oven, or game shows. Initially this device was based on an electromechanical system which was identical to an electric bell without the metal gong (which makes the ringing noise).

piezo buzzers are used across many major industries as a means for audible identification or alert. From extremely compact 4 mm SMT buzzers to larger, high decibel models, this product family is well suited to address the needs of the most challenging audio alert applications.



**FEATURES:**

* Rated Voltage: Max 30 Vp-p
* Current Consumption: 12mA @ 10Vp-p Square Wave 4.1kHz
* Sound Pressure Level(10cm): 90dB @ 10Vp-p Square Wave 4.1kHz
* Flying Leads Fitted
* High and Clear Sound, audible for many metres - KPE-110
* Dimensions: 24mm Diameter, 5mm High, 29mm between mounting holes

**4. RELAY**

A relay is an electrically operated switch. Current flowing through the coil of the relay creates a magnetic field which attracts a lever and changes the switch contacts. The coil current can be on or off so relays have two switch positions and they are double throw (changeover) switches.

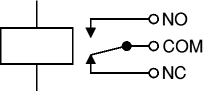
Relays allow one circuit to switch a second circuit which can be completely separate from the first. For example a low voltage battery circuit can use a relay to switch a 230V AC mains circuit. There is no electrical connection inside the relay between the two circuits, the link is magnetic and mechanical.

Relays are very simple devices. There are four major parts in every realy. They are

* Electromagnet
* Armature that can be attracted by the electromagnet
* Spring
* Set of electrical contacts

**4.1 WORKING**

When a current flows through the coil, the resulting magnetic field attracts an armature that is mechanically linked to a moving contact. The movement either makes or breaks a connection with a fixed contact. When the current to the coil is switched off, the armature is returned by a force approximately half as strong as the magnetic force to its relaxed position. Usually this is a spring, but gravity is also used commonly in industrial motor starters. Most relays are manufactured to operate quickly. In a low voltage application, this is to reduce noise. In a high voltage or high current application, this is to reduce arcing.



**Fig 8.1 Circuit symbol of a relay**

The relay's switch connections are usually labeled COM, NC and NO:

* COM = Common, always connect to this, it is the moving part of the switch.
* NC = Normally Closed, COM is connected to this when the relay coil is off.
* NO = Normally Open, COM is connected to this when the relay coil is on.

**NOTE:**Connect to COM and NO if you want the switched circuit to be on when the relay coil is on. Connect to COM and NC if you want the switched circuit to be on when the relay coil is off.

**4.2 ADVANTAGES OF RELAYS**

Like relays, transistors can be used as an electrically operated switch. For switching small DC currents (< 1A) at low voltage they are usually a better choice than a relay. However transistors cannot switch AC or high voltages (such as mains electricity) and they are not usually a good choice for switching large currents (> 5A). In these cases a relay will be needed. Advantages of relays compared to other switching devices are:

* The complete electrical isolation improves safety by ensuring that high voltages and currents cannot appear where they should not be.
* Relays can switch many contacts at once. Relays come in all shapes and sizes for different applications and they have various switch contact configurations.  Double Pole Double Throw (DPDT) relays are common and even 4-pole types are available.  You can therefore control several circuits with one relay or use one relay to control the direction of a motor.
* Relays can switch AC and DC, transistors can only switch DC.
* Relays can switch high voltages, transistors cannot.
* Relays are a better choice for switching large currents (> 5A).

**4.3 DRIVE CIRCUIT AND PROTECTION DIODES FOR RELAYS**

### The coil of a relay passes a relatively large current, typically 30mA for a 12V relay, but it can be as much as 100mA for relays designed to operate from lower voltages. Hence a CB amplifier is used to achieve the current rating of the relay.

Transistors and ICs must be protected from the brief high voltage produced when a relay coil is switched off. The diagram shows how a signal diode (e.g. 1N4148) is connected 'backwards' across the relay coil to provide this protection.

Current flowing through a relay coil creates a magnetic field which collapses suddenly when the current is switched off. The sudden collapse of the magnetic field induces a brief high voltage across the relay coil which is very likely to damage transistors and ICs. The protection diode allows the induced voltage to drive a brief current through the coil (and diode) so the magnetic field dies away quickly rather than instantly. This prevents the induced voltage becoming high enough to cause damage to transistors and ICs.

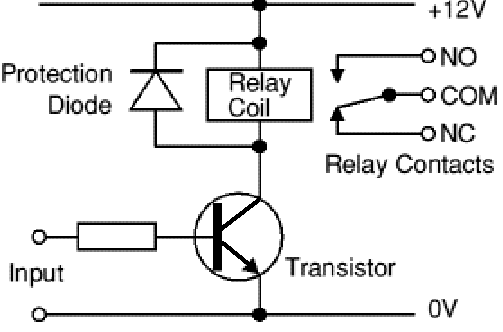


Fig 8.2 Drive circuit and protection diodes for relays

**4.4 CHOOSING A RELAY:**

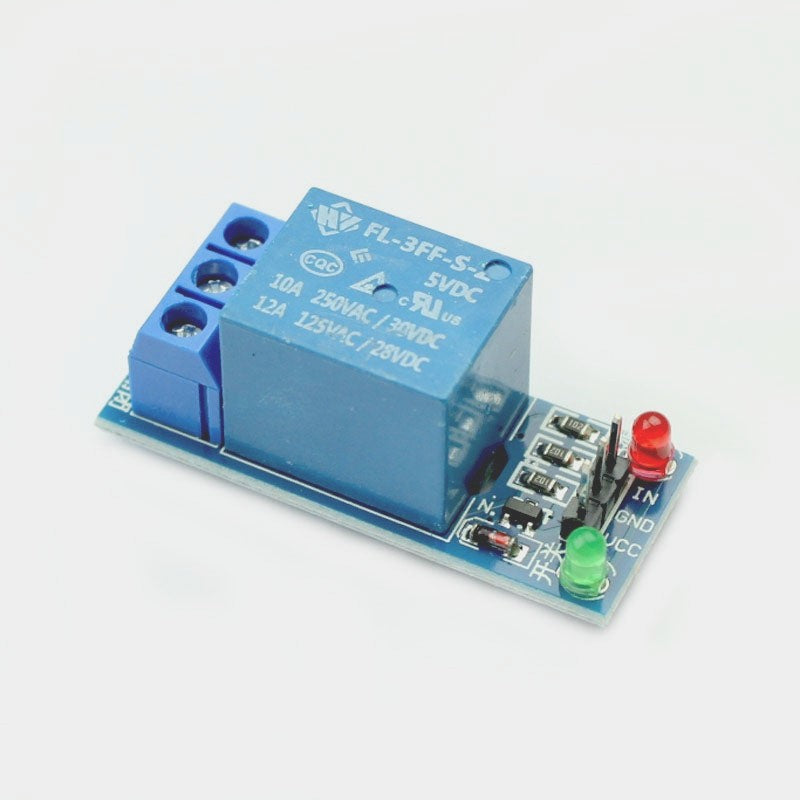
### One needs to consider several features when choosing a relay:

1. **Physical size and pin arrangement:** If you are choosing a relay for an existing PCB you will need to ensure that its dimensions and pin arrangement are suitable. You should find this information in the supplier's catalogue.
2. **Coil voltage:** The relay's coil voltage rating and resistance must suit the circuit powering the relay coil. Many relays have a coil rated for a 12V supply but 5V and 24V relays are also readily available. Some relays operate perfectly well with a supply voltage which is a little lower than their rated value.
3. **Coil resistance:** The circuit must be able to supply the current required by the relay coil. You can use Ohm's law to calculate the current:

Relay coil current   =   supply voltage / coil resistance

For example: A 12V supply relay with a coil resistance of 400ohm passes a current of 30mA. Most ICs will require a transistor to amplify the current.

1. **Switch ratings (voltage and current):** The relay's switch contacts must be suitable for the circuit they are to control. You will need to check the voltage and current ratings. Note that the voltage rating is usually higher for AC, for example: "5A at 24V DC or 125V AC".
2. **Switch contact arrangement (SPDT, DPDT etc.):** Most relays are SPDT or DPDT which are often described as "single pole changeover" (SPCO) or "double pole changeover" (DPCO).



**5. DC MOTOR**

A **DC motor** is any of a class of rotary [electrical motors](https://en.wikipedia.org/wiki/Electrical_motor) that converts direct current (DC) electrical energy into mechanical energy. The most common types rely on the forces produced by magnetic fields. Nearly all types of DC motors have some internal mechanism, either electromechanical or electronic, to periodically change the direction of current in part of the motor.

DC motors were the first form of motor widely used, as they could be powered from existing direct-current lighting power distribution systems. A DC motor's speed can be controlled over a wide range, using either a variable supply voltage or by changing the strength of current in its field windings. Small DC motors are used in tools, toys, and appliances. The [universal motor](https://en.wikipedia.org/wiki/Universal_motor) can operate on direct current but is a lightweight [brushed](https://en.wikipedia.org/wiki/Brush_(electric)) motor used for portable power tools and appliances. Larger DC motors are currently used in propulsion of electric vehicles, elevator and hoists, and in drives for steel rolling mills. The advent of [power electronics](https://en.wikipedia.org/wiki/Power_electronics) has made replacement of DC motors with [AC motors](https://en.wikipedia.org/wiki/AC_motors) possible in many applications.

**DESCRIPTION**

DC motors are rotary electrical machines that convert electrical energy into mechanical energy (Rotation).

**SPECIFICATION**

* Speed : 2000RPM
* Voltage : 5V

**APPLICATIONS**

* Automatic products
* Motorized toys
* Hair Dryer
* Hand made vaccum cleaner



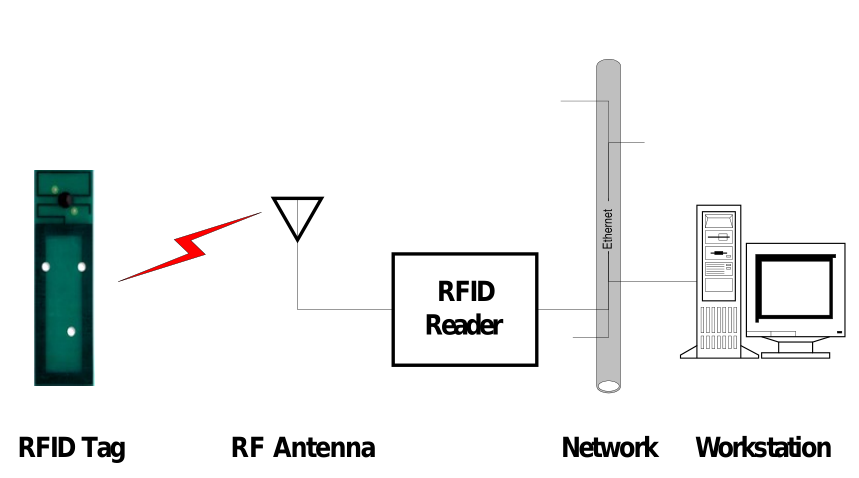
**RFID Reader**

RFID  is a Radio Frequency IDentification.

An ADC (Automated Data Collection) technology that:

* uses radio­frequency waves to transfer data between a reader and a movable item to identify, categorize, track..
* Is fast and does not require physical sight or contact between reader/scanner and the tagged item.
* Performs the operation using low cost components.
* Attempts to provide unique identification and backend integration that allows for wide range of applications.

Other ADC technologies: Bar codes, OCR.



**RFID TAGS:**

**Tags can be attached to almost anything:**

* Items, cases or pallets of products, high value goods
* vehicles, assets, livestock or personnel

**Passive Tags**

* Do not require power – Draws from Interrogator Field
* Lower storage capacities (few bits to 1 KB)
* Shorter read ranges (4 inches to 15 feet)
* Usually Write­Once­Read­Many/Read­Only tags
* Cost around 25 cents to few dollars

**Active Tags**

* Battery powered
* Higher storage capacities (512 KB)
* Longer read range (300 feet)
* Typically can be re­written by RF Interrogators
* Cost around 50 to 250 dollars



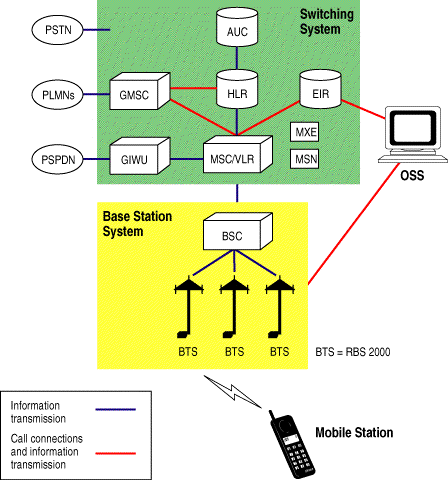
**GSM MODEM:**

DEFINITION:

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz.

**7.6.2 THE GSM NETWORK**

GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers. The GSM network is divided into three major systems: the switching system (SS), the base station system (BSS), and the operation and support system (OSS). The basic GSM network elements are shown in below figure



**GSM Network Elements**

**7.6.3 GSM MODEM:**

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves.

A GSM modem can be an external device or a PC Card / PCMCIA Card. Typically, an external GSM modem is connected to a computer through a serial cable or a USB cable. A GSM modem in the form of a PC Card / PCMCIA Card is designed for use with a laptop computer. It should be inserted into one of the PC Card / PCMCIA Card slots of a laptop computer. Like a GSM mobile phone, a GSM modem requires a SIM card from a wireless carrier in order to operate.

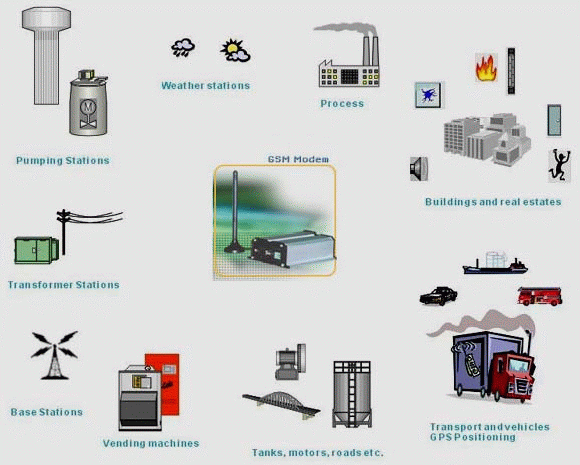
As mentioned in earlier sections of this SMS tutorial, computers use AT commands to control modems. Both GSM modems and dial-up modems support a common set of standard AT commands. You can use a GSM modem just like a dial-up modem.

In addition to the standard AT commands, GSM modems support an extended set of AT commands. These extended AT commands are defined in the GSM standards. With the extended AT commands, you can do things like:

* Reading, writing and deleting SMS messages.
* Sending SMS messages.
* Monitoring the signal strength.
* Monitoring the charging status and charge level of the battery.
* Reading, writing and searching phone book entries.

The number of SMS messages that can be processed by a GSM modem per minute is very low -- only about six to ten SMS messages per minute.

**7.6.4 GSM MODEM APPLICATIONS:**



**7.6.5 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  
  
**7.6.6 APPLICATIONS:**

**Access control devices:**

Now access control devices can communicate with servers and security staff through SMS messaging. Complete log of transaction is available at the head-office Server instantly without any wiring involved and device can instantly alert security personnel on their mobile phone in case of any problem. RaviRaj Technologies is introducing this technology in all Fingerprint Access control and time attendance products.

**Transaction terminals:**

EDC machines, POS terminals can use SMS messaging to confirm transactions from central servers. The main benefit is that central server can be anywhere in the world. Today you need local servers in every city with multiple telephone lines. You save huge infrastructure costs as well as per transaction cost.

**Supply Chain Management:**

Today SCM require huge IT infrastructure with leased lines, networking devices, data centre, workstations and still you have large downtimes and high costs. You can do all this at a fraction of the cost with GSM M2M technology. A central server in your head office with GSM capability is the answer; you can receive instant transaction data from all your branch officers, warehouses and business associates with nil downtime, Low cost

**7.7 APPLICATIONS SUITABLE FOR GSM COMMUNICATION:**

If your application needs one or more of the following features, GSM will be more cost-effective then other communication systems.

**Short Data Size:**

You data size per transaction should be small like 1-3 lines. e.g. banking transaction data, sales/purchase data, consignment tracking data, updates. These small but important transaction data can be sent through SMS messaging which cost even less then a local telephone call or sometimes free of cost worldwide. Hence with negligible cost you are able to send critical information to your head office located anywhere in the world from multiple points.

You can also transfer faxes, large data through GSM but this will be as or more costly compared to landline networks.

**Multiple remote data collection points:**

If you have multiple data collections points situated all over your city, state, country or worldwide you will benefit the most. The data can be sent from multiple points like your branch offices, business associates, warehouses, and agents with devices like GSM modems connected to PCs, GSM electronic terminals and Mobile phones. Many a times some places like warehouses may be situated at remote location may not have landline or internet but you will have GSM network still available easily.

**High uptime:**

If your business require high uptime and availability GSM is best suitable for you as GSM mobile networks have high uptime compared to landline, internet and other communication mediums. Also in situations where you expect that someone may sabotage your communication systems by cutting wires or taping landlines, you can depend on GSM wireless communication.  
  
**Large transaction volumes:**

GSM SMS messaging can handle large number of transaction in a very short time. You can receive large number SMS messages on your server like e-mails without internet connectivity. E-mails normally get delayed a lot but SMS messages are almost instantaneous for instant transactions. Consider situation like shop owners doing credit card transaction with GSM technology instead of conventional landlines. time you find local transaction servers busy as these servers use multiple telephone lines to take care of multiple transactions, whereas one GSM connection is enough to handle hundreds of transaction.

**Mobility, Quick installation:**

GSM technology allows mobility, GSM terminals, modems can be just picked and installed at other location unlike telephone lines. Also you can be mobile with GSM terminals and can also communicate with server using your mobile phone. You can just purchase the GSM hardware like modems, terminals and mobile handsets, insert SIM cards, configure software and your are ready for GSM communication.

**SOFTWARE DESCRIPTION**

1. **PYTHON PROGRAMMING**

**Python** is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. It was created by Guido van Rossum during 1985- 1990. Like Perl, Python source code is also available under the GNU General Public License (GPL). This **tutorial** gives enough understanding on **Python programming** language.

## Why to Learn Python?

**Python** is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages.

**Python** is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain. I will list down some of the key advantages of learning Python:

**Python is Interpreted** − Python is processed at runtime by the interpreter. You do not need to compile your program before executing it. This is similar to PERL and PHP.

**Python is Interactive** − You can actually sit at a Python prompt and interact with the interpreter directly to write your programs.

**Python is Object-Oriented** − Python supports Object-Oriented style or technique of programming that encapsulates code within objects.

**Python is a Beginner's Language** − Python is a great language for the beginner-level programmers and supports the development of a wide range of applications from simple text processing to WWW browsers to games.

## Characteristics of Python

Following are important characteristics of **Python Programming** −

It supports functional and structured programming methods as well as OOP.

It can be used as a scripting language or can be compiled to byte-code for building large applications.

It provides very high-level dynamic data types and supports dynamic type checking.

It supports automatic garbage collection.

It can be easily integrated with C, C++, COM, ActiveX, CORBA, and Java.

## Hello World using Python.

Just to give you a little excitement about Python, I'm going to give you a small conventional Python Hello World program, You can try it using Demo link.

[Live Demo](http://tpcg.io/4nOH9K)

print ("Hello, Python!");

## Applications of Python

As mentioned before, Python is one of the most widely used language over the web. I'm going to list few of them here:

**Easy-to-learn** − Python has few keywords, simple structure, and a clearly defined syntax. This allows the student to pick up the language quickly.

**Easy-to-read** − Python code is more clearly defined and visible to the eyes.

**Easy-to-maintain** − Python's source code is fairly easy-to-maintain.

**A broad standard library** − Python's bulk of the library is very portable and cross-platform compatible on UNIX, Windows, and Macintosh.

**Interactive Mode** − Python has support for an interactive mode which allows interactive testing and debugging of snippets of code.

**Portable** − Python can run on a wide variety of hardware platforms and has the same interface on all platforms.

**Extendable** − You can add low-level modules to the Python interpreter. These modules enable programmers to add to or customize their tools to be more efficient.

**Databases** − Python provides interfaces to all major commercial databases.

**GUI Programming** − Python supports GUI applications that can be created and ported to many system calls, libraries and windows systems, such as Windows MFC, Macintosh, and the X Window system of Unix.

**Scalable** − Python provides a better structure and support for large programs than shell scripting.

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages.

**Python is Interpreted** − Python is processed at runtime by the interpreter. You do not need to compile your program before executing it. This is similar to PERL and PHP.

**Python is Interactive** − You can actually sit at a Python prompt and interact with the interpreter directly to write your programs.

**Python is Object-Oriented** − Python supports Object-Oriented style or technique of programming that encapsulates code within objects.

**Python is a Beginner's Language** − Python is a great language for the beginner-level programmers and supports the development of a wide range of applications from simple text processing to WWW browsers to games.

## History of Python

Python was developed by Guido van Rossum in the late eighties and early nineties at the National Research Institute for Mathematics and Computer Science in the Netherlands.

Python is derived from many other languages, including ABC, Modula-3, C, C++, Algol-68, SmallTalk, and Unix shell and other scripting languages.

Python is copyrighted. Like Perl, Python source code is now available under the GNU General Public License (GPL).

Python is now maintained by a core development team at the institute, although Guido van Rossum still holds a vital role in directing its progress.

## Python Features

Python's features include −

**Easy-to-learn** − Python has few keywords, simple structure, and a clearly defined syntax. This allows the student to pick up the language quickly.

**Easy-to-read** − Python code is more clearly defined and visible to the eyes.

**Easy-to-maintain** − Python's source code is fairly easy-to-maintain.

**A broad standard library** − Python's bulk of the library is very portable and cross-platform compatible on UNIX, Windows, and Macintosh.

**Interactive Mode** − Python has support for an interactive mode which allows interactive testing and debugging of snippets of code.

**Portable** − Python can run on a wide variety of hardware platforms and has the same interface on all platforms.

**Extendable** − You can add low-level modules to the Python interpreter. These modules enable programmers to add to or customize their tools to be more efficient.

**Databases** − Python provides interfaces to all major commercial databases.

**GUI Programming** − Python supports GUI applications that can be created and ported to many system calls, libraries and windows systems, such as Windows MFC, Macintosh, and the X Window system of Unix.

**Scalable** − Python provides a better structure and support for large programs than shell scripting.

Apart from the above-mentioned features, Python has a big list of good features, few are listed below −

It supports functional and structured programming methods as well as OOP.

It can be used as a scripting language or can be compiled to byte-code for building large applications.

It provides very high-level dynamic data types and supports dynamic type checking.

It supports automatic garbage collection.

It can be easily integrated with C, C++, COM, ActiveX, CORBA, and Java.

A module allows you to logically organize your Python code. Grouping related code into a module makes the code easier to understand and use. A module is a Python object with arbitrarily named attributes that you can bind and reference.

Simply, a module is a file consisting of Python code. A module can define functions, classes and variables. A module can also include runnable code.

## Example

The Python code for a module named *aname* normally resides in a file named *aname.py*. Here's an example of a simple module, support.py

def print\_func( par ):

print "Hello : ", par

return

## The *import* Statement

You can use any Python source file as a module by executing an import statement in some other Python source file. The *import* has the following syntax −

import module1[, module2[,... moduleN]

When the interpreter encounters an import statement, it imports the module if the module is present in the search path. A search path is a list of directories that the interpreter searches before importing a module. For example, to import the module support.py, you need to put the following command at the top of the script −

#!/usr/bin/python

# Import module supportimport support

# Now you can call defined function that module as follows

support.print\_func("Zara")

When the above code is executed, it produces the following result −

Hello : Zara

A module is loaded only once, regardless of the number of times it is imported. This prevents the module execution from happening over and over again if multiple imports occur.

## The *from...import* Statement

Python's *from* statement lets you import specific attributes from a module into the current namespace. The *from...import* has the following syntax −

from modname import name1[, name2[, ... nameN]]

For example, to import the function fibonacci from the module fib, use the following statement −

from fib import fibonacci

This statement does not import the entire module fib into the current namespace; it just introduces the item fibonacci from the module fib into the global symbol table of the importing module.

## The *from...import \** Statement

It is also possible to import all names from a module into the current namespace by using the following import statement −

from modname import \*

This provides an easy way to import all the items from a module into the current namespace; however, this statement should be used sparingly.

## Locating Modules

When you import a module, the Python interpreter searches for the module in the following sequences −

The current directory.

If the module isn't found, Python then searches each directory in the shell variable PYTHONPATH.

If all else fails, Python checks the default path. On UNIX, this default path is normally /usr/local/lib/python/.

The module search path is stored in the system module sys as the **sys.path** variable. The sys.path variable contains the current directory, PYTHONPATH, and the installation-dependent default.

## The *PYTHONPATH* Variable

The PYTHONPATH is an environment variable, consisting of a list of directories. The syntax of PYTHONPATH is the same as that of the shell variable PATH.

Here is a typical PYTHONPATH from a Windows system −

set PYTHONPATH = c:\python20\lib;

And here is a typical PYTHONPATH from a UNIX system −

set PYTHONPATH = /usr/local/lib/python

## Namespaces and Scoping

Variables are names (identifiers) that map to objects. A *namespace* is a dictionary of variable names (keys) and their corresponding objects (values).

A Python statement can access variables in a *local namespace* and in the *global namespace*. If a local and a global variable have the same name, the local variable shadows the global variable.

Each function has its own local namespace. Class methods follow the same scoping rule as ordinary functions.

Python makes educated guesses on whether variables are local or global. It assumes that any variable assigned a value in a function is local.

Therefore, in order to assign a value to a global variable within a function, you must first use the global statement.

The statement *global VarName* tells Python that VarName is a global variable. Python stops searching the local namespace for the variable.

For example, we define a variable *Money* in the global namespace. Within the function *Money*, we assign *Money* a value, therefore Python assumes *Money* as a local variable. However, we accessed the value of the local variable *Money* before setting it, so an UnboundLocalError is the result. Uncommenting the global statement fixes the problem.

#!/usr/bin/python

Money = 2000def AddMoney():

# Uncomment the following line to fix the code:

# global Money

Money = Money + 1

print MoneyAddMoney()print Money

## The dir( ) Function

The dir() built-in function returns a sorted list of strings containing the names defined by a module.

The list contains the names of all the modules, variables and functions that are defined in a module. Following is a simple example −

[Live Demo](http://tpcg.io/ZoifUr)

#!/usr/bin/python

# Import built-in module mathimport math

content = dir(math)print content

When the above code is executed, it produces the following result −

['\_\_doc\_\_', '\_\_file\_\_', '\_\_name\_\_', 'acos', 'asin', 'atan',

'atan2', 'ceil', 'cos', 'cosh', 'degrees', 'e', 'exp',

'fabs', 'floor', 'fmod', 'frexp', 'hypot', 'ldexp', 'log',

'log10', 'modf', 'pi', 'pow', 'radians', 'sin', 'sinh',

'sqrt', 'tan', 'tanh']

Here, the special string variable *\_\_name\_\_* is the module's name, and *\_\_file\_\_* is the filename from which the module was loaded.

## The *globals()* and *locals()* Functions

The *globals()* and *locals()* functions can be used to return the names in the global and local namespaces depending on the location from where they are called.

If locals() is called from within a function, it will return all the names that can be accessed locally from that function.

If globals() is called from within a function, it will return all the names that can be accessed globally from that function.

The return type of both these functions is dictionary. Therefore, names can be extracted using the keys() function.

## The *reload()* Function

When the module is imported into a script, the code in the top-level portion of a module is executed only once.

Therefore, if you want to reexecute the top-level code in a module, you can use the *reload()* function. The reload() function imports a previously imported module again. The syntax of the reload() function is this −

reload(module\_name)

Here, *module\_name* is the name of the module you want to reload and not the string containing the module name. For example, to reload *hello* module, do the following −

reload(hello)

## Packages in Python

A package is a hierarchical file directory structure that defines a single Python application environment that consists of modules and subpackages and sub-subpackages, and so on.

Consider a file *Pots.py* available in *Phone* directory. This file has following line of source code −

#!/usr/bin/python

def Pots():

print "I'm Pots Phone"

Similar way, we have another two files having different functions with the same name as above −

*Phone/Isdn.py* file having function Isdn()

*Phone/G3.py* file having function G3()

Now, create one more file \_\_init\_\_.py in *Phone* directory −

Phone/\_\_init\_\_.py

To make all of your functions available when you've imported Phone, you need to put explicit import statements in \_\_init\_\_.py as follows −

from Pots import Pots

from Isdn import Isdn

from G3 import G3

After you add these lines to \_\_init\_\_.py, you have all of these classes available when you import the Phone package.

#!/usr/bin/python

# Now import your Phone Package.import Phone

Phone.Pots()Phone.Isdn()Phone.G3()

When the above code is executed, it produces the following result −

I'm Pots Phone

I'm 3G Phone

I'm ISDN Phone

In the above example, we have taken example of a single functions in each file, but you can keep multiple functions in your files. You can also define different Python classes in those files and then you can create your packages out of those classes.

Simple Mail Transfer Protocol (SMTP) is a protocol, which handles sending e-mail and routing e-mail between mail servers.

Python provides **smtplib** module, which defines an SMTP client session object that can be used to send mail to any Internet machine with an SMTP or ESMTP listener daemon.

Here is a simple syntax to create one SMTP object, which can later be used to send an e-mail −

import smtplib

smtpObj = smtplib.SMTP( [host [, port [, local\_hostname]]] )

Here is the detail of the parameters −

**host** − This is the host running your SMTP server. You can specify IP address of the host or a domain name like tutorialspoint.com. This is optional argument.

**port** − If you are providing *host* argument, then you need to specify a port, where SMTP server is listening. Usually this port would be 25.

**local\_hostname** − If your SMTP server is running on your local machine, then you can specify just *localhost* as of this option.

An SMTP object has an instance method called **sendmail**, which is typically used to do the work of mailing a message. It takes three parameters −

The *sender* − A string with the address of the sender.

The *receivers* − A list of strings, one for each recipient.

The *message* − A message as a string formatted as specified in the various RFCs

1. **OPEN CV**

**Classification of images :-**

There are 3 types of images used in image processing. They are,

1. Binary image
2. Gray scale image
3. Color image.
4. **BINARY IMAGE :**

In binary image two colours are used. Typically the two colors used for a binary image two colors are black and white. Binary image is also called a two-level. Each pixel is stored as a single bit 0 or 1. 0 is represented as black and 1 is defined as white. In digital image processing binary operation mainly used in segmentation, thresholding, and dithering. Some input/output devices, fax machines and bi-level computer displays can handle a bi-level images.

**2 . GRAY SCALE IMAGE :**

A grayscale image is digital image. For grayscale images, the result is a two-dimensional array with the number of rows and columns in image. Low numeric values indicate darker shades and higher values lighter shades. The range of pixel values is often 0 to 255. We divide by 255 to get a range of 0 to 1.

Gray images have many shades of gray in between . gray scale images also called as a monochromatic, denoting the absence of any chromatic variations. Gray scale images are most commonly used in image processing because smaller data enables developers to do more complex operations in a shorter time.

**3 . COLOUR IMAGE** **:**

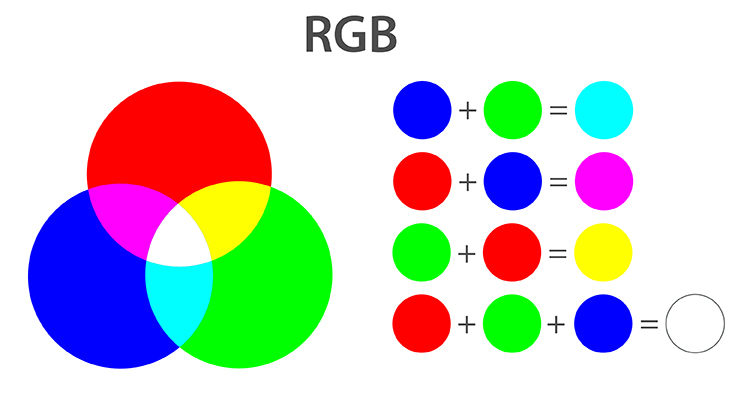
A color image has three colours or three channels in per pixel . They measure the intensity and chrominance of light. A color image is typically represented by a bit depth ranging from 8 to 24 or higher.  the bits are often divided into three groupings: 8 for red, 8 for green, and 8 for blue. The decomposition of a color in the three prilimary colors is quantified by a number between o and 255.

Example,

White will be defined as R=255, G =255, B =255.

Black will be defines as R=0 ,G =0, B =0.

The secondary colors: magenta (red+blue), cyan (green+blue), and yellow (red+green).



**BASIC OF IMAGE PROCESSING :**

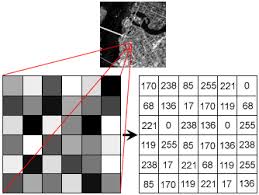
1. **IMAGE :**

An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows. Image is a two-dimensional, such as a photograph, screen display, and as well as three-dimensional such a statue. They may be captured by optical devices – such as cameras, mirrors , lenses, telescopes, microscopes, etc.

1. **Pixel :**

A pixel is generally thought of as the smallest single component of a digital image**.** ... For example, there can be "printed pixels" in a page

pixels carried by electronic signals, or represented by digital values, or pixels on a display device, or pixels in a digital camera (photosensor elements). In digital imaging, a pixel(or picture element) is **the smallest item of information in an image**. Pixels are arranged in a 2-dimensional grid, represented using squares. Each pixel is a sample of an original image, where more samples typically provide more-accurate representations of the original.

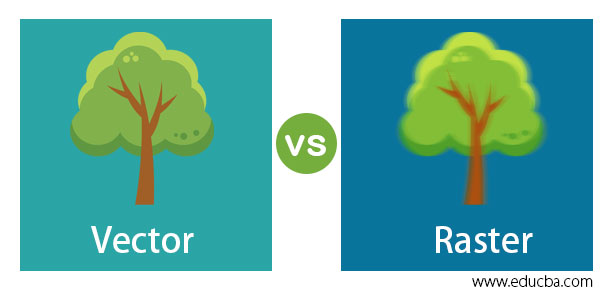
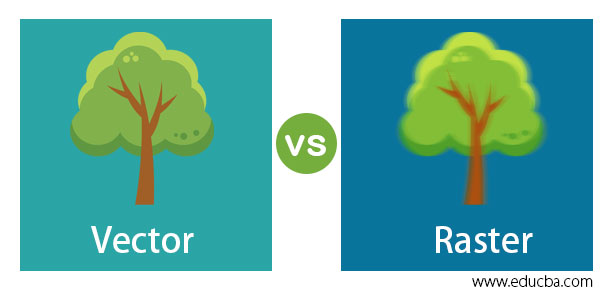


Each pixel has a color. The color is a 32-bit integer

First eight bit determine the red pixels, next eight pixel determine the green pixel, next eight pixel determine the blue pixel and remaining eight bits the transparency of the pixel.

1. **IMAGE FILE FORMATS**:

Including proprietary types, there are hundreds of image file types. The **PNG, JPEG, and GIF formats** are most often used to display images on the Internet. Some of these graphic formats are listed and briefly described below, separated into the two main families of graphics: raster and vector.



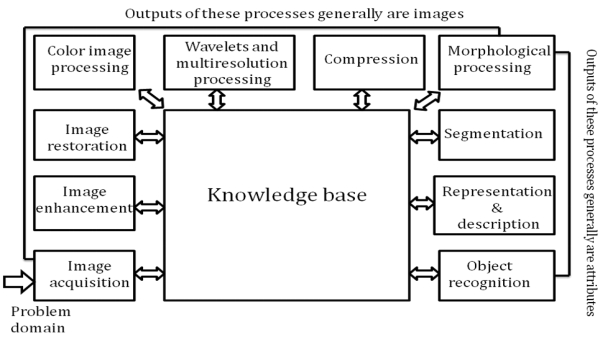
**IMAGE PROCESSING :**

Image processing is **a method to perform some operations on an image**, in order to get an enhanced image or to extract some useful information from it. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image.

The inherent subjective appeal of pictorial displays attracts perhaps a disproportionate amount of attention from the scientist and also form a layman. Digital image processing like other glamour fields, suffers from myths, misconnections, misunderstandings.

Several factor combine to indicate a lively future for digital image processing. A major factor is declining cost of computer equipment. Several new technologies trends promote digital image processing. These include parallel processing mode practical by low cost microprocessors ,and the use of the charge coupled devices for digitizing, storage during processing and display and large low cost microprocessors, and the use of charge coupled devices (CCDs) for digitizing, storage during processing and display and large low cost of image storage arrays.

**FUNDAMENTAL STEPS IN DIGITAL IMAGE PROCESSING:**



**Image Acquisition:**

**Image Acquisition** is to acquire a digital image. To do so requires an image sensor and the capability to digitize the signal produced by the sensor. The sensor could be monochrome or color TV camera that produces an entire image of the problem domain every 1/30 sec. the image sensor could also be line scan camera that produces a single image line at a time. In this case, the objects motion past the line.



Scanner produces a two-dimensional image. If the output of the camera or other imaging sensor is not in digital form, an analog to digital converter digitizes it. The nature of the sensor and the image it produces are determined by the application.



**Image Enhancement :**

**Image enhancement**is among the simplest and most appealing areas of digital image processing. Basically, the idea behind enhancement techniques is to bring out detail that is obscured, or simply to highlight certain features of interesting an image. A familiar example of enhancement is when we increase the contrast of an image because “it looks better.” It is important to keep in mind that enhancement is a very subjective area of image processing.



**Image restoration:**

**Image restoration**is an area that also deals with improving the appearance of an image. However, unlike enhancement, which is subjective, image restoration is objective, in the sense that restoration techniques tend to be based on mathematical or probabilistic models of image degradation.



Enhancement, on the other hand, is based on human subjective preferences regarding what constitutes a “good” enhancement result. For example, contrast stretching is considered an enhancement technique because it is based primarily on the pleasing aspects it might present to the viewer, where as removal of image blur by applying a deblurring function is considered a restoration technique.

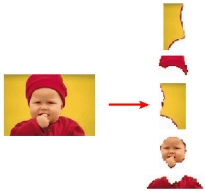
**Color image processing:**

The use of color in image processing is motivated by two principal factors. First, color is a powerful descriptor that often simplifies object identification and extraction from a scene. Second, humans can discern thousands of color shades and intensities, compared to about only two dozen shades of gray. This second factor is particularly important in manual image analysis.



**Segmentation:**

**Segmentation**procedures partition an image into its constituent parts or objects. In general, autonomous segmentation is one of the most difficult tasks in digital image processing. A rugged segmentation procedure brings the process a long way toward successful solution of imaging problems that require objects to be identified individually.



On the other hand, weak or erratic segmentation algorithms almost always guarantee eventual failure. In general, the more accurate the segmentation, the more likely recognition is to succeed.

Digital image is defined as a two dimensional function f(x, y), where x and y are spatial (plane) coordinates, and the amplitude of f at any pair of coordinates (x, y) is called intensity or grey level of the image at that point. The field of digital image processing refers to processing digital images by means of a digital computer. The digital image is composed of a finite number of elements, each of which has a particular location and value. The elements are referred to as picture elements, image elements, pels, and pixels. Pixel is the term most widely used.

**Image Compression**

Digital Image compression addresses the problem of reducing the amount of data required to represent a digital image. The underlying basis of the reduction process is removal of redundant data. From the mathematical viewpoint, this amounts to transforming a 2D pixel array into a statically uncorrelated data set. The data redundancy is not an abstract concept but a mathematically quantifiable entity. If n1 and n2 denote the number of information-carrying units in two data sets that represent the same information, the relative data redundancy C:\Users\ELCOT\AppData\Local\Temp\ksohtml\wpsB9A5.tmp.png [2] of the first data set (the one characterized by n1) can be defined as,

C:\Users\ELCOT\AppData\Local\Temp\ksohtml\wpsB9A6.tmp.png

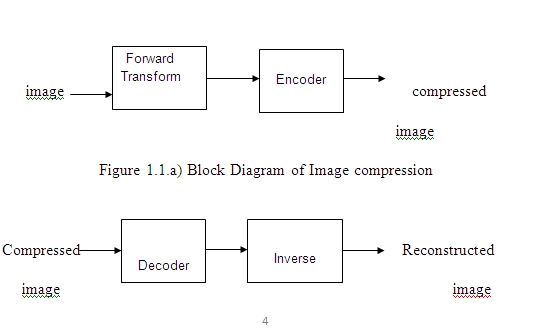
Where C:\Users\ELCOT\AppData\Local\Temp\ksohtml\wps4FFC.tmp.png called as compression ratio [2]. It is defined as

C:\Users\ELCOT\AppData\Local\Temp\ksohtml\wps4FFD.tmp.png= C:\Users\ELCOT\AppData\Local\Temp\ksohtml\wps4FFE.tmp.png

In image compression, three basic data redundancies can be identified and exploited: Coding redundancy, interpixel redundancy, and phychovisal redundancy. Image compression is achieved when one or more of these redundancies are reduced or eliminated.

The image compression is mainly used for image transmission and storage. Image transmission applications are in broadcast television; remote sensing via satellite, air-craft, radar, or sonar; teleconferencing; computer communications; and facsimile transmission. Image storage is required most commonly for educational and business documents, medical images that arise in computer tomography (CT), magnetic resonance imaging (MRI) and digital radiology, motion pictures, satellite images, weather maps, geological surveys, and so on.

**Image Compression Model**



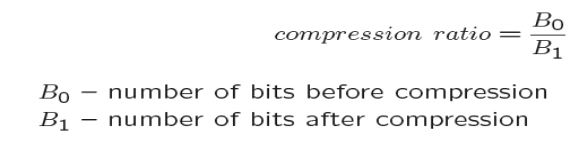
**Image Compression Type:**

There are two types’ image compression techniques.

1. Lossy Image compression

2. Lossless Image compression

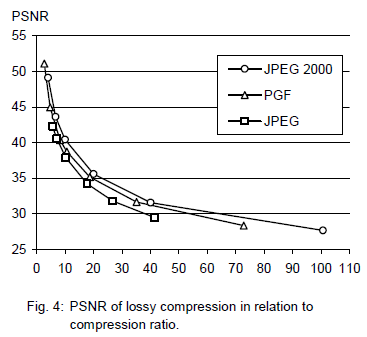
Compression ratio:



1. **Lossy Image compression :**

Lossy compression means that **the image size is reduced while some data** from the original image file is eliminated. The lossy image process is irreversible. Once you have compressed an image this way, you can't go back.

Lossy compression provides higher levels of data reduction but result in a less than perfect reproduction of the original image. It provides high compression ratio. lossy image compression is useful in applications such as broadcast television, videoconferencing, and facsimile transmission, in which a certain amount of error is an acceptable trade-off for increased compression performance.



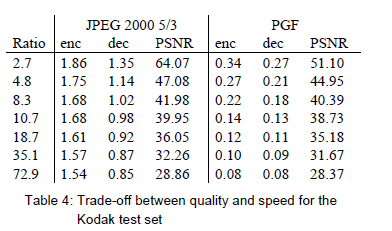
In the next test series we evaluate the lossy compression efficiency of PGF. One of the best competitors in this area is for sure JPEG 2000. Since JPEG 2000 has two different filters, we used the one with the better trade-off between compression efficiency and runtime. On our machine the 5/3 filter set has a better trade-off than the other. However, JPEG 2000 has in both cases a remarkable good compression efficiency for very high compression ratios but also a very poor encoding and decoding speed.

The other competitor is JPEG. JPEG is one of the most popular image file formats. It is very fast and has a reasonably good compression efficiency for a wide range of compression ratios. The drawbacks of JPEG are the missing lossless compression and the often missing progressive decoding.

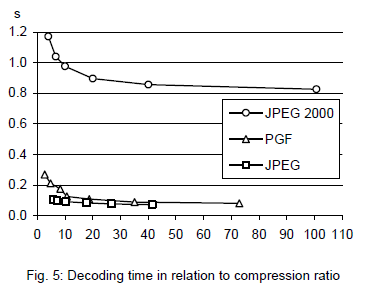
These results are also qualitative valid for our PGF test set and they are characteristic for aerial ortho-photos and natural images. Because of the design of PGF we already know that PGF does not reach the compression efficiency of JPEG 2000. However, we are interested in the trade-off between compression efficiency and runtime. To report this trade-off we show in Table 4 a comparison between JPEG 2000 and PGF and in Fig. 5 (on page 8) we show for the same test series as in Fig. 4 the corresponding average decoding times in relation to compression ratios.

Table 4 contains for seven different compression ratios (mean values over the compression ratios of the eight images of the Kodak test set) the corresponding average encoding and decoding times in relation to the average PSNR values. In case of PGF the encoding time is always slightly longer than the corresponding decoding time. The reason for that is that the actual encoding phase (cf. Subsection 2.4.2) takes slightly longer than the corresponding decoding phase.

For six of seven ratios the PSNR difference between JPEG 2000 and PGF is within 3% of the PSNR of JPEG 2000. Only in the first row is the difference larger (21%), but because a PSNR of 50 corresponds to an almost perfect image quality the large PSNR difference corresponds with an almost undiscoverable visual difference. The price they pay in JPEG 2000 for the 3% more PSNR is very high. The creation of a PGF is five to twenty times faster than the creation of a corresponding JPEG 2000 file, and the decoding of the created PGF is still five to ten times faster than the decoding of the JPEG 2000 file. This gain in speed is remarkable, especially in areas where time is more important than quality, maybe for instance in real-time computation.



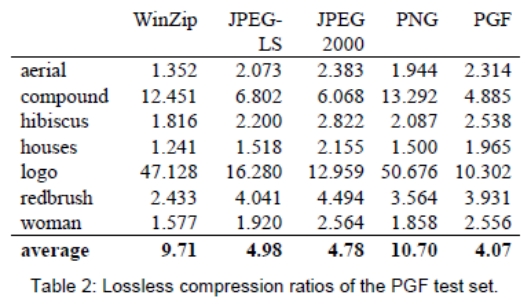
In Fig. 5 we see that the price we pay in PGF for the 3% more PSNR than JPEG is low: for small compression ratios (< 9) decoding in PGF takes two times longer than JPEG and for higher compression ratios (> 30) it takes only ten percent longer than JPEG. These test results are characteristic for both natural images and aerial ortho-photos. Again, in the third test series we only use the ‘Lena’ image. We run our lossy coder with six different quantization parameters and measure the PSNR in relation to the resulting compression ratios. The results (ratio: PSNR) are:



**2.Lossless Image compression :**

Lossless Image compression is useful in applications such as medical imaginary, business documents and satellite images.

Table summarizes the lossless compression efficiency and Table 3 the coding times of the PGF test set. For WinZip we only provide average runtime values, because of missing source code we have to use an interactive testing procedure with runtimes measured by hand. All other values are measured in batch mode



In Table 2 it can be seen that in almost all cases the best compression ratio is obtained by JPEG 2000, followed by PGF, JPEG-LS, and PNG. This result is different to the result in [SEA+00], where the best performance for a similar test set has been reported for JPEG-LS. PGF performs between 0.5% (woman) and 21.3% (logo) worse than JPEG 2000. On average it is almost 15% worse. The two exceptions to the general trend are the ‘compound’ and the ‘logo’ images. Both images contain for the most part black text on a white background. For this type of images, JPEG-LS and in particular WinZip and PNG provide much larger compression ratios. However, in average PNG performs the best, which is also reported in [SEA+00].

These results show, that as far as lossless compression is concerned, PGF performs reasonably well on natural and aerial images. In specific types of images such as ‘compound’ and ‘logo’ PGF is outperformed by far in PNG.

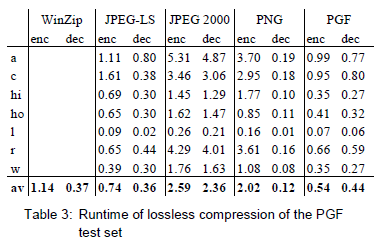


Table 3 shows the encoding (enc) and decoding (dec) times (measured in seconds) for the same algorithms and images as in Table 2. JPEG 2000 and PGF are both symmetric algorithms, while WinZip, JPEG-LS and in particular PNG are asymmetric with a clearly shorter decoding than encoding time. JPEG 2000, the slowest in encoding and decoding, takes more than four times longer than PGF. This speed gain is due to the simpler coding phase of PGF. JPEG-LS is slightly slower than PGF during encoding, but slightly faster in decoding images.

WinZip and PNG decode even more faster than JPEG-LS, but their encoding times are also worse. PGF seems to be the best compromise between encoding and decoding times. Our PGF test set clearly shows that PGF in lossless mode is best suited for natural images and aerial orthophotos. PGF is the only algorithm that encodes the three MByte large aerial ortho-photo in less than second without a real loss of compression efficiency. For this particular image the efficiency loss is less than three percent compared to the best. These results should be underlined with our second test set, the Kodak test set.

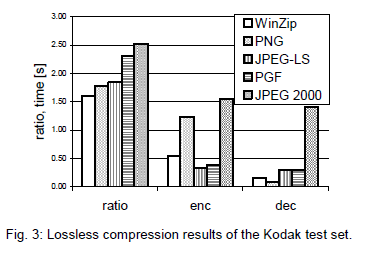


Fig. 3 shows the averages of the compression ratios (ratio), encoding (enc), and decoding (dec) times over all eight images. JPEG 2000 shows in this test set the best compression efficiency followed by PGF, JPEG-LS, PNG, and WinZip. In average PGF is eight percent worse than JPEG 2000. The fact that JPEG 2000 has a better lossless compression ratio than PGF does not surprise, because JPEG 2000 is more quality driven than PGF.

However, it is remarkable that PGF is clearly better than JPEG-LS (+21%) and PNG (+23%) for natural images. JPEG-LS shows in the Kodak test set also a symmetric encoding and decoding time behavior. Its encoding and decoding times are almost equal to PGF. Only PNG and WinZip can faster decode than PGF, but they also take longer than PGF to encode.

If both compression efficiency and runtime is important, then PGF is clearly the best of the tested algorithms for lossless compression of natural images and

aerial orthophotos. In the third test we perform our lossless coder on the ‘Lena’ image. The compression ratio is 1.68 and the encoding and decoding takes 0.25 and 0.19 seconds, respectively.

**Image Compression Standards**

There are many methods available for lossy and lossless, image compression. The efficiency of these coding standardized by some Organizations. The International Standardization Organization (ISO) and Consultative Committee of the International Telephone and Telegraph (CCITT) are defined the image compression standards for both binary and continuous tone (monochrome and Colour) images. Some of the Image Compression Standards are,

1. JBIG1

2. JBIG2

3. JPEG-LS

4. DCT based JPEG

5. Wavelet based JPEG2000

**CONCLUSION**

`This project can overcome the issue of impersonation of a cardholder. This is like a two factor authentication method which is used to confirm that the transaction is done by the card owner or the persons trusted by the owner using face recognition. It limits the card usage of the unauthorized users who hold the password of someone’s card. Thus, this ATM model provides security against exploitation of identity, by using a verification system using face recognition to the identity and confirm the user and it will scale back forced transactions to an excellent extent.

Nowadays, the ATM robberies are common. In this proposal, a real-time monitoring system for ATM security based on accelerometer sensor, camera module, and fingerprint module is proposed. The proposed work concludes with the following points. Itis a secure way of accessing an ATM by authorized persons using face recognition module. Eliminates the drawback of previous system like manual controlling camera modules and doors the system is cost effective as compare to existing manual technique. The live video of the ATM centre can be monitored through web server which make ATM better safe from thefts. This is completely accessed through card holder and it is one of the major advantages of this proposed system. However, this system has some disadvantages which can’t be a major risk but it has to be considered. Fingerprint won’t work when it is wet or wounded. Sometimes finger print module may won’t work properly. Such kinds of issues are there but in general this system offers better security than before proposed systems.

**FUTURE ENHANCEMENTS**

As we mentioned, facial recognition technique seems more challenging as compared to other biometrics, thus more efficient algorithm can be developed. The flaws in face recognition technique like the inability to detect face when beard, aging, glasses and caps can be rectified and eliminated or reduced. If the cost of retina or iris recognition reduces, it can be used instead of face recognition.

As facial recognition technique seems more challenging as compared to other biometrics, thus more efficient algorithm can be developed. The inability to detect face when beard and aging can be rectified and eliminated or reduced. Instead of face recognition retinal or iris recognition can be used if the cost is reduced.

**REFERENCES**

* Abdulmajeed, Alsufyani1, Alroobaea1, Ahmed, Roobaea, Detection of single-trial EEG of the neural correlates of familiar faces recognition using machinelearning algorithms, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.6, November – December 2019, pp.2855-2860.
* Aru, O.Ezeand I.Gozie, Facial Verification Technology for Use in ATM Transactions, in American Journal of Engineering Research (AJER), [Online] 2013, pp. 188-193. https://doi.org/10.30534/ijatcse/2019/28862019
* Babaei, O.Molalapata and A.A.Pandor, Face Recognition Application for Automatic Teller Machines (ATM), in ICIKM, 3rdvol.45, November – December 2012, pp.211-216.
* Derman, Y.K.Gecici and A.A.Salah, Short Term Face Recognition for Automatic Teller Machine (ATM) Users, in ICECCO 2013, Istanbul, Turkey, pp.111-114. https://dx.doi.org/10.21172/1.841.20
* JinfangXu, Khan, Rasib and RasibHasan, SEPIA: Secure-PIN-authentication-as-a-service for ATM using Mobile and wearable devices, 3 rdIEEE International Conference on Mobile Cloud Computing, Services, and Engineering IEEE, June 2015,pp. 41-50.
* Marilou O. Espina1, Arnel C. Fajardo, Bobby D. Gerardo, RujiP. Medina, Multiple Level Information Security Using Image Steganography and Authentication, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.6, November – December 2019, pp.3297-3303. https://doi.org/10.30534/ijatcse/2019/100862019
* Murugesan, R.Elankeerthana, Support vector machine the most fruitful algorithm for prognosticating heart disorder , International, Journal of Engineering and Technology, Volume 7, pp.48 – 52, 2018. https://doi.org/10.14419/ijet.v7i2.26.12533
* Murugesan,S.Thilagamani, Overview Of Techniques For Face Recognition, International Journal Of Life Science and Pharma Reviews , pp.66 - 71 , 2019 , ISSN 2250 – 0480. https://dx.doi.org/10.22376/ijpbs/10.SP01/Oct/2019
* Murugesan, R.Elankeerthana, Pedestrian ReIdentification Using Deep Learning, International Journal Of Life Science and Pharma Reviews, pp.71 - 78 , 2019 , ISSN 2250 – 0480.
* Pandiaraja, N. Deepa, A Novel Data PrivacyPreserving Protocol for Multi-data Users by using genetic algorithm, Journal Soft Computing Volume 23 Issue 18, pp8539-8553, 2019.
* Karthikeyan, S.Sainath, K.P.TharunAswin, K.Abimanyu, An Automated Anti-Theft and Misusealerting System for ATM, IOSR Journal of Electronics and Communication Engineering (IOSRJECE), Volume 10, Issue 2, Ver. II (Mar - Apr.2015), PP 97-102.
* RajeshKanna, P.Pandiaraja, An Efficient Sentiment Analysis Approach for Product Review using Turney Algorithm, Journal of Procedia, Computer Science ,Volume 165, Issue 2019, PP 356-362. https://doi.org/10.1016/j.procs.2020.01.038
* Sri Vasu, Subash, Sharmila Rani, Udhayakumar,ATM Security using Machine Learning techniques in IOT, International Journal of Advance Research, Ideas and Innovations in Technology, Volume 5, Issue 2, pp. 150- 153, 2019.
* Thilagamani , N. Shanthi, Object Recognition Based on Image Segmentation and Clustering, Journal of Computer Science, Vol.7, No.11, pp. 1741-1748, 2011. https://doi.org/10.3844/jcssp.2011.1741.1748
* Daniel Peralta, Mikel Galar, Isaac Triguero, Oscar Miguel-Hurtado, Jose M. Benitez, and Francisco Herrera, “Minutiae filtering to improve both efficacy and efficiency of fingerprint matching algorithms,” Engineering Applications of Artificial Intelligence, June 2014, Volume 32, Pages 37- 53.
* Balwir, K.R. Katole, R.D. Thakare, N.S. Panchbudhe, and P.K. Balwir, "Secured ATM Transaction System Using Micro-Controller", International Journal of Advanced Research in Computer Science and Software Engineering, April 2014, vol. 4, no. 4, pp. 1358-1362.
* Bharati M Nelligani, Dr. N V Uma Reddy, and Mr.NithinAwasti, “Smart ATM Security System Using FPR, GSM, GPS”, International Conference on Inventive Computation Technologies (ICICT), 26-27 Aug. 2016.
* Guru Sarath, “Centralized Server Based ATM Security System with Statistical Vulnerability Prediction Capability,” IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 2017, pp.61-66.
* Sweta Singh, Akhilesh Singh, and Rakesh Kumar, “A Constraint based Biometric Scheme on ATM and Swiping Machine,” International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016
* Akhilesh Singh, Sweta Singh, and Rakesh Kumar,” Secure Swipe Machine with Help of Biometric Security,” International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp.1056-1061.
* Renee Jebaline, and S. Gomathi, “A Novel Method to Enhance the Security of ATM using Biometrics,” International Conference on Circuit, Power and Computing Technologies [ICCPCT], 2015.
* Vengatesan, Rohit Ravindra Nikam, S. Yuvaraj,Ankoshe Malakappa Shankar, Punjabi Shivkumar Tanesh and Abhishek Kumar"A Random Forest-based Classification Method for Prediction of Car Price",International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 03, 2020.
* Dr. Mohammed Aref, Dr. Sameen Ahmed Khan,Dr. Sayyad Samee, K. Vengatesan and Abhishek Kumar," Early Detection of Outbreaks by Monitoring the Over-the-Counter Pharmacy Sales" International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 04, 2020.
* Ambeth Kumar, ∗, S. Malathia, R. Venkatesan, K. Ramalakshmi, K. Vengatesan, Weiping Ding and Abhishek Kumar,"Exploration of an innovative geometric parameter based on performance enhancement for foot print recognition",Journal of Intelligent & Fuzzy Systems.
* Saravana Kumar, E., Vengatesan, K. Trust based resource selection with optimization technique. Cluster Comput 22, 207–213 (2019)
* Prabu, S., V. Balamurugan, and K. Vengatesan. "Design of cognitive image filters for suppression of noise level in medical images." Measurement 141 (2019): 296-301.
* Jignesh J. Patoliya, and Miral M. Desai, “Face detection-based ATM Security system using embedded Linux platform”, 2nd International Conference for Convergence in Technology (I2CT), 2017, pp 74-78
* Akyildiz, and K.L. Bernhardt, "ATM Local Area Networks, ASurvey of Requirements, Architectures, and Standards", IEEE Communications Magazine, July 1997, vol. 35, no. 7, pp. 72- 80.