INPUT DEVICE

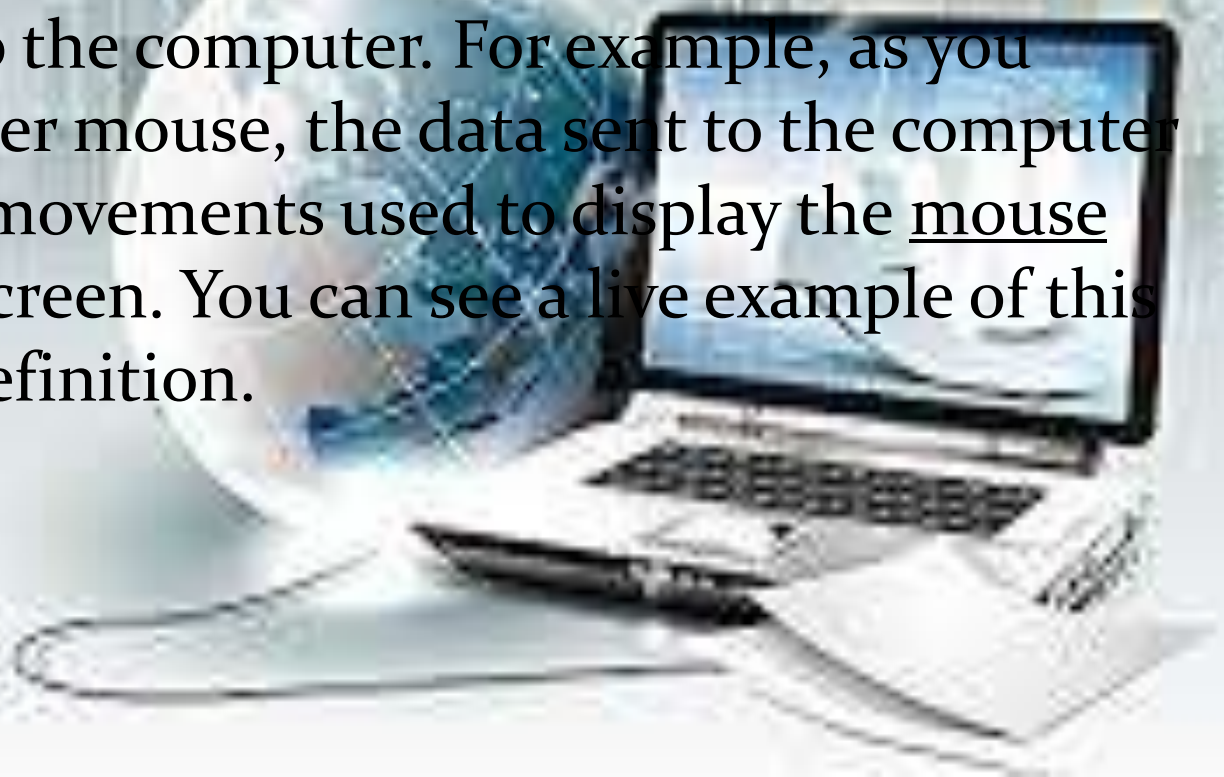
Mrs. A. KALAISELVI
Assistant Professor,
Department of computer Science,
Arul Anandar college Karumathur.

What are the input devices of my computer?

- Every computer has a keyboard and a mouse (touchpad with laptop), considered input devices. As far as other input devices, it depends on what was included with your computer and what's connected. The best method of determining your computer's input devices is to go through the above list with the types of input devices.

What does an input device send to a computer?

- What an input device sends (inputs) to a computer depends on the device. Additionally, all input devices send data from the device over a cable or wireless transmission to the computer. For example, as you move a computer mouse, the data sent to the computer is the X-Y axis movements used to display the mouse cursor on the screen. You can see a live example of this on our x-axis definition.



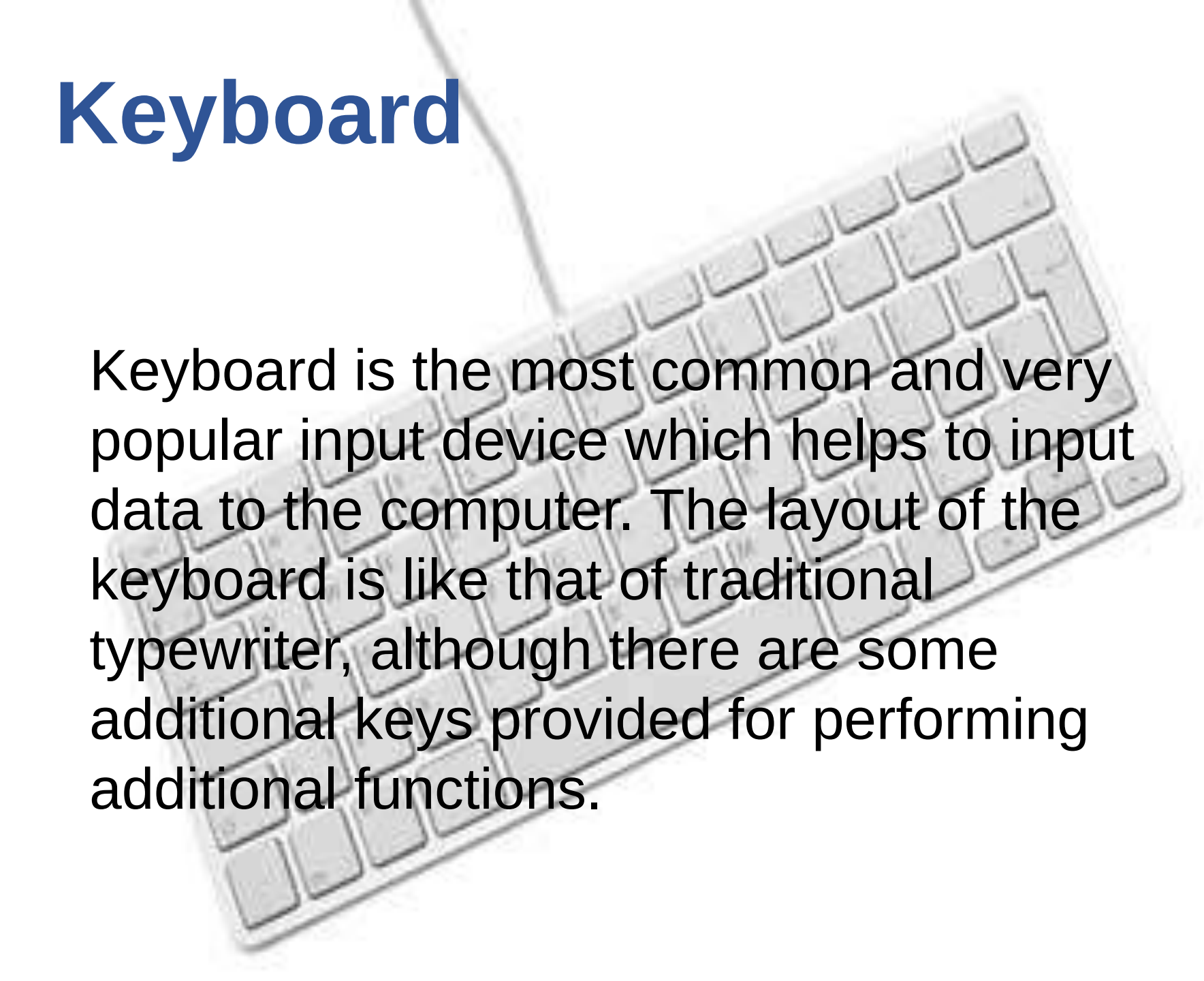
Why does a computer need an input device?

- Today, input devices are important because they let you interact with and add new information to a computer. For example, if a computer had no input devices, it could run by itself, but there would be no way to change its settings, fix errors, or other various user interactions. Also, if you wanted to add new information to the computer (e.g., text, command, document, picture, etc.), you wouldn't be able to do so without an input device.

Following are some of the important input devices which are used in a computer

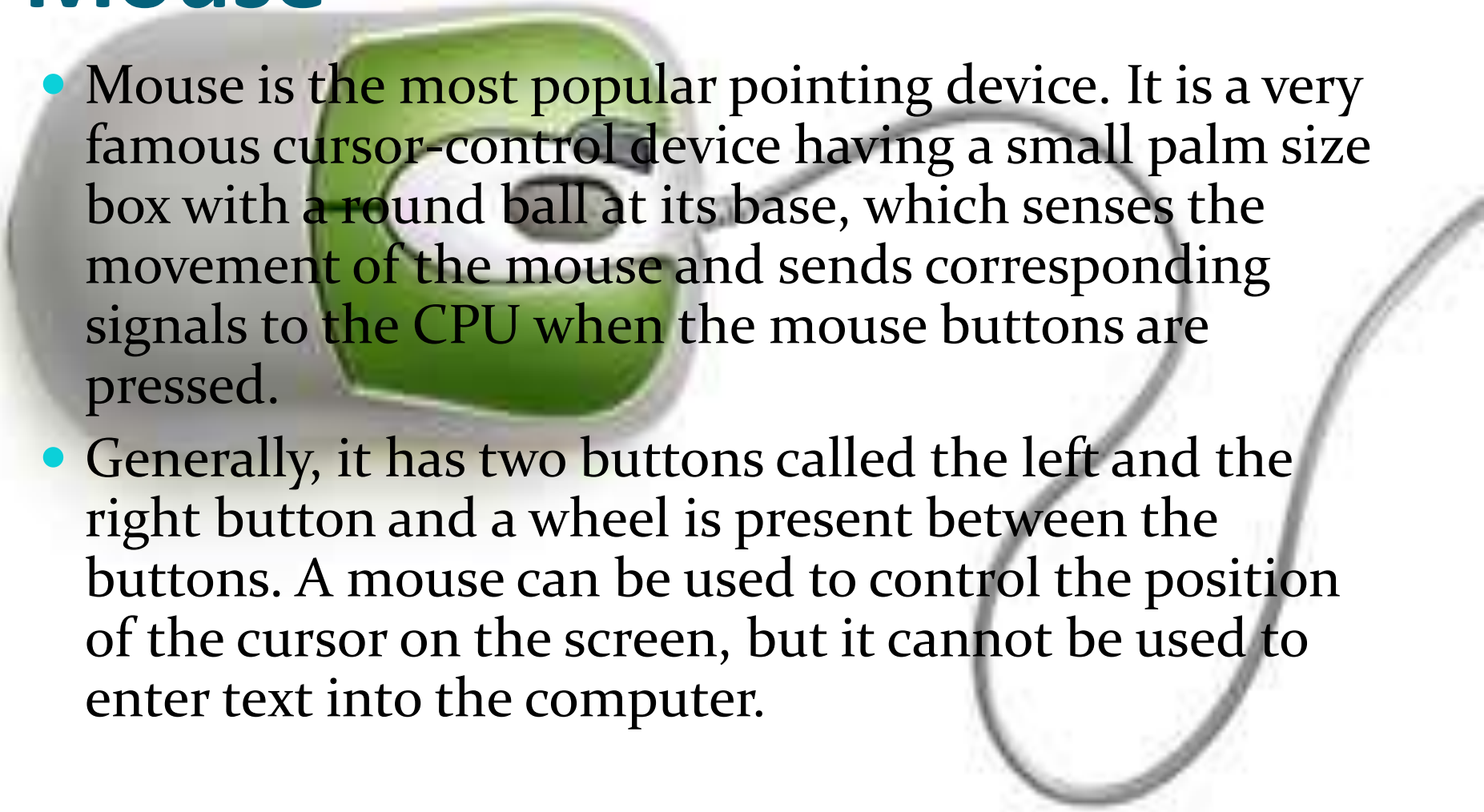
- Keyboard
- Mouse
- Joy Stick
- Light Pen
- Track Ball
- Scanner
- Graphic Tablet
- Microphone
- Magnetic Ink Card Reader(MICR)
- Optical Character Reader(OCR)
- Bar Code Reader
- Optical Mark Reader(OMR)

Keyboard



Keyboard is the most common and very popular input device which helps to input data to the computer. The layout of the keyboard is like that of traditional typewriter, although there are some additional keys provided for performing additional functions.

Mouse

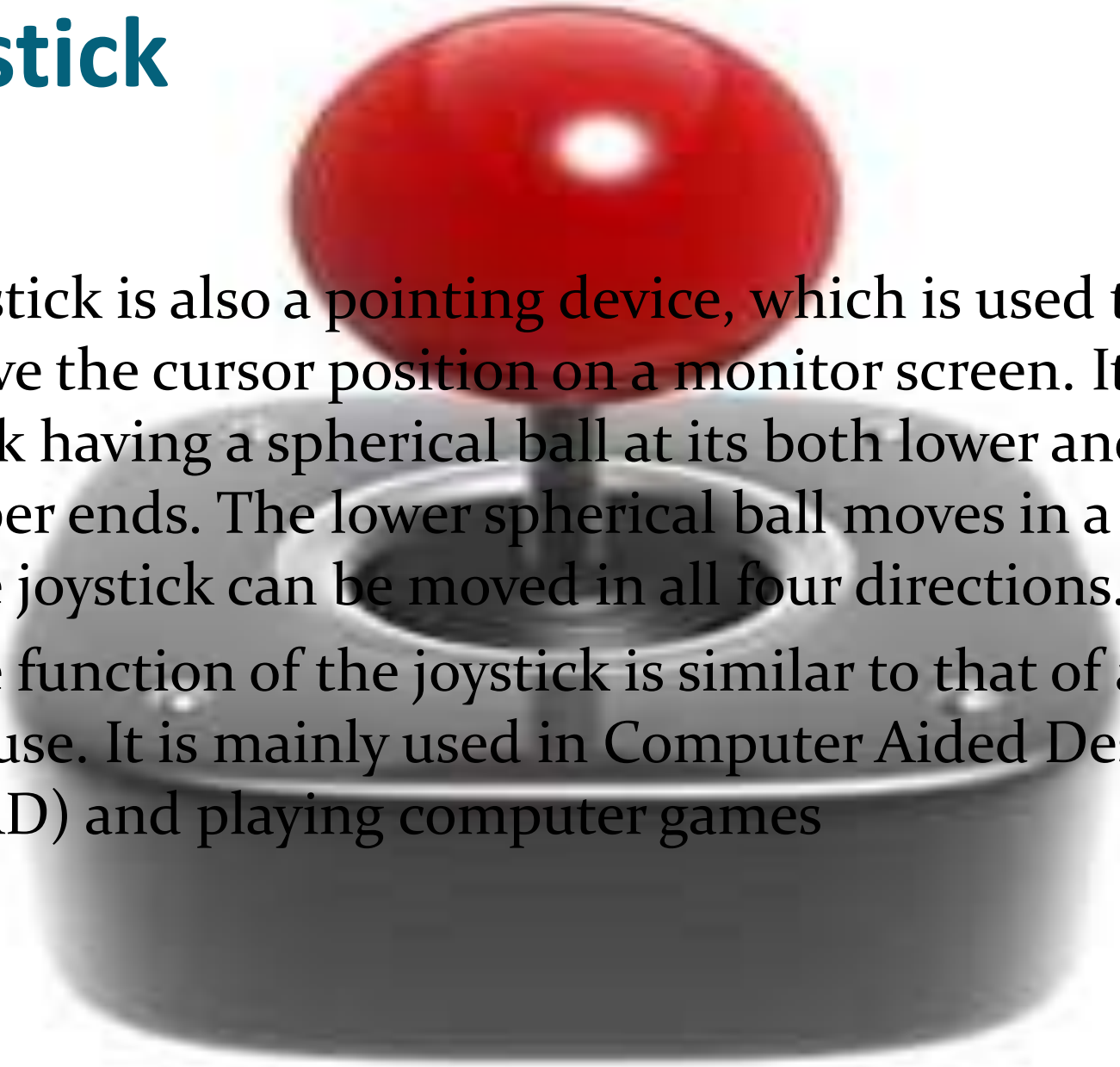


- Mouse is the most popular pointing device. It is a very famous cursor-control device having a small palm size box with a round ball at its base, which senses the movement of the mouse and sends corresponding signals to the CPU when the mouse buttons are pressed.
- Generally, it has two buttons called the left and the right button and a wheel is present between the buttons. A mouse can be used to control the position of the cursor on the screen, but it cannot be used to enter text into the computer.

Advantages

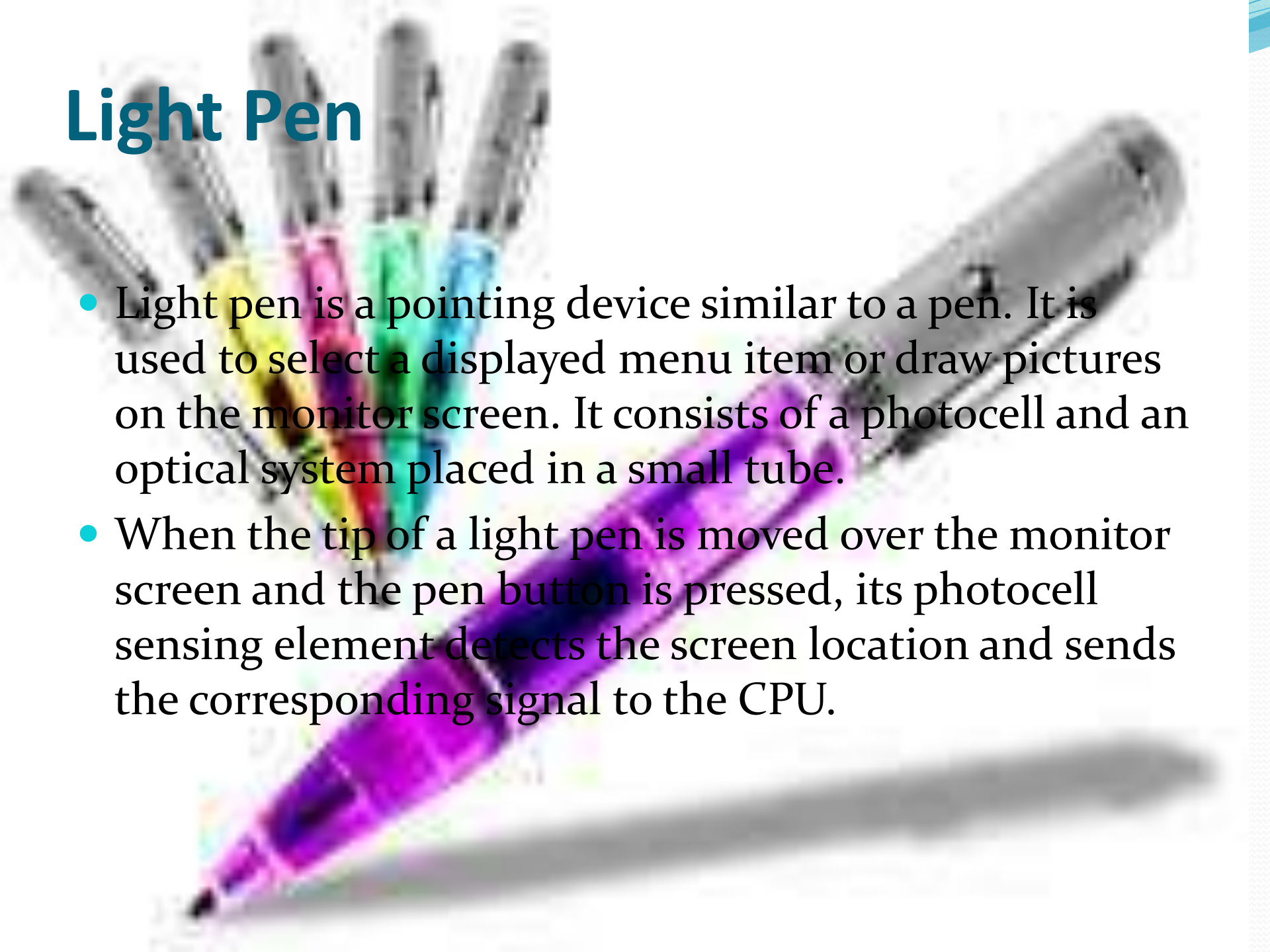
- Easy to use
- Not very expensive
- Moves the cursor faster than the arrow keys of the keyboard.

Joystick



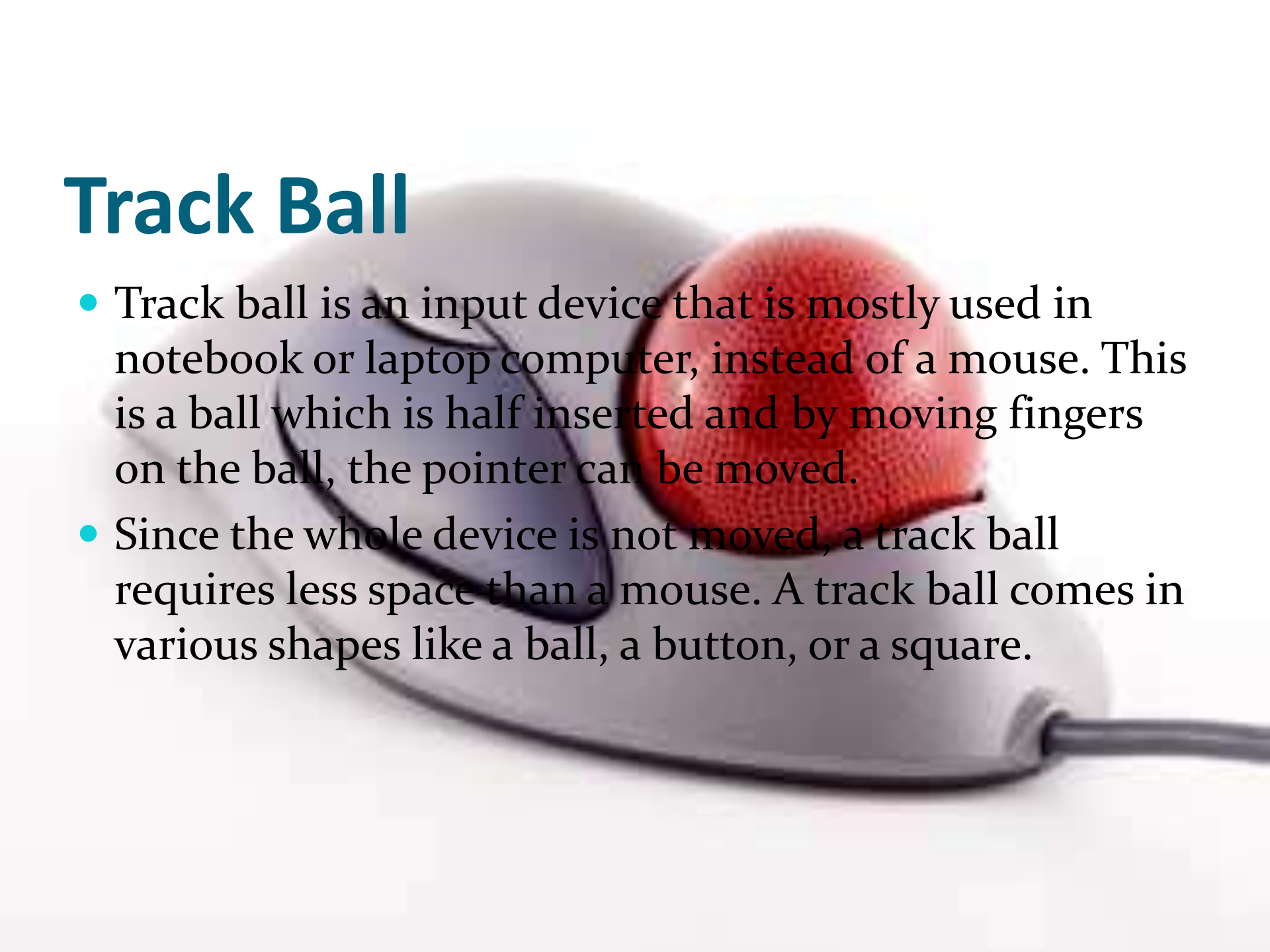
- Joystick is also a pointing device, which is used to move the cursor position on a monitor screen. It is a stick having a spherical ball at its both lower and upper ends. The lower spherical ball moves in a socket. The joystick can be moved in all four directions.
- The function of the joystick is similar to that of a mouse. It is mainly used in Computer Aided Designing (CAD) and playing computer games

Light Pen



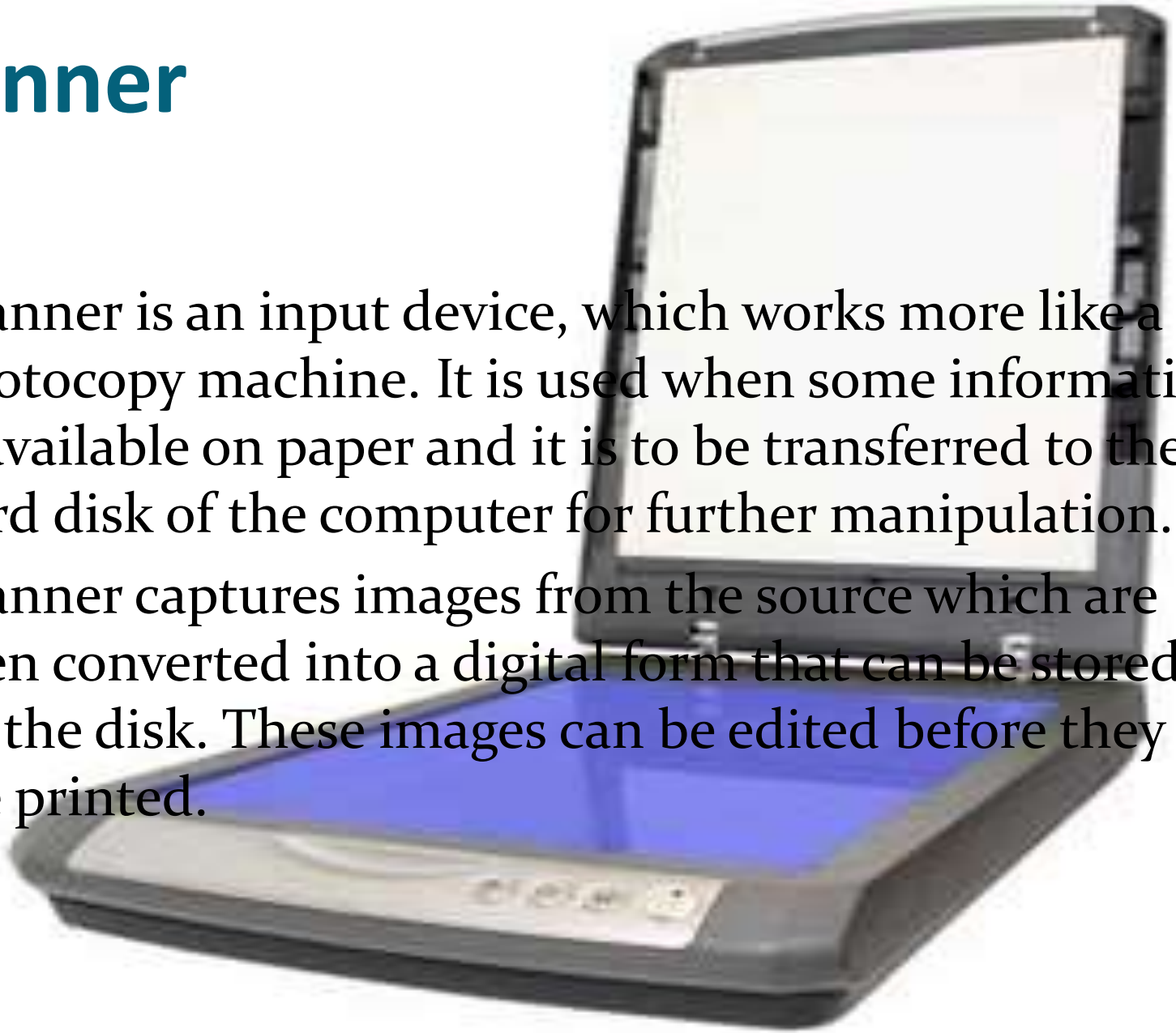
- Light pen is a pointing device similar to a pen. It is used to select a displayed menu item or draw pictures on the monitor screen. It consists of a photocell and an optical system placed in a small tube.
- When the tip of a light pen is moved over the monitor screen and the pen button is pressed, its photocell sensing element detects the screen location and sends the corresponding signal to the CPU.

Track Ball



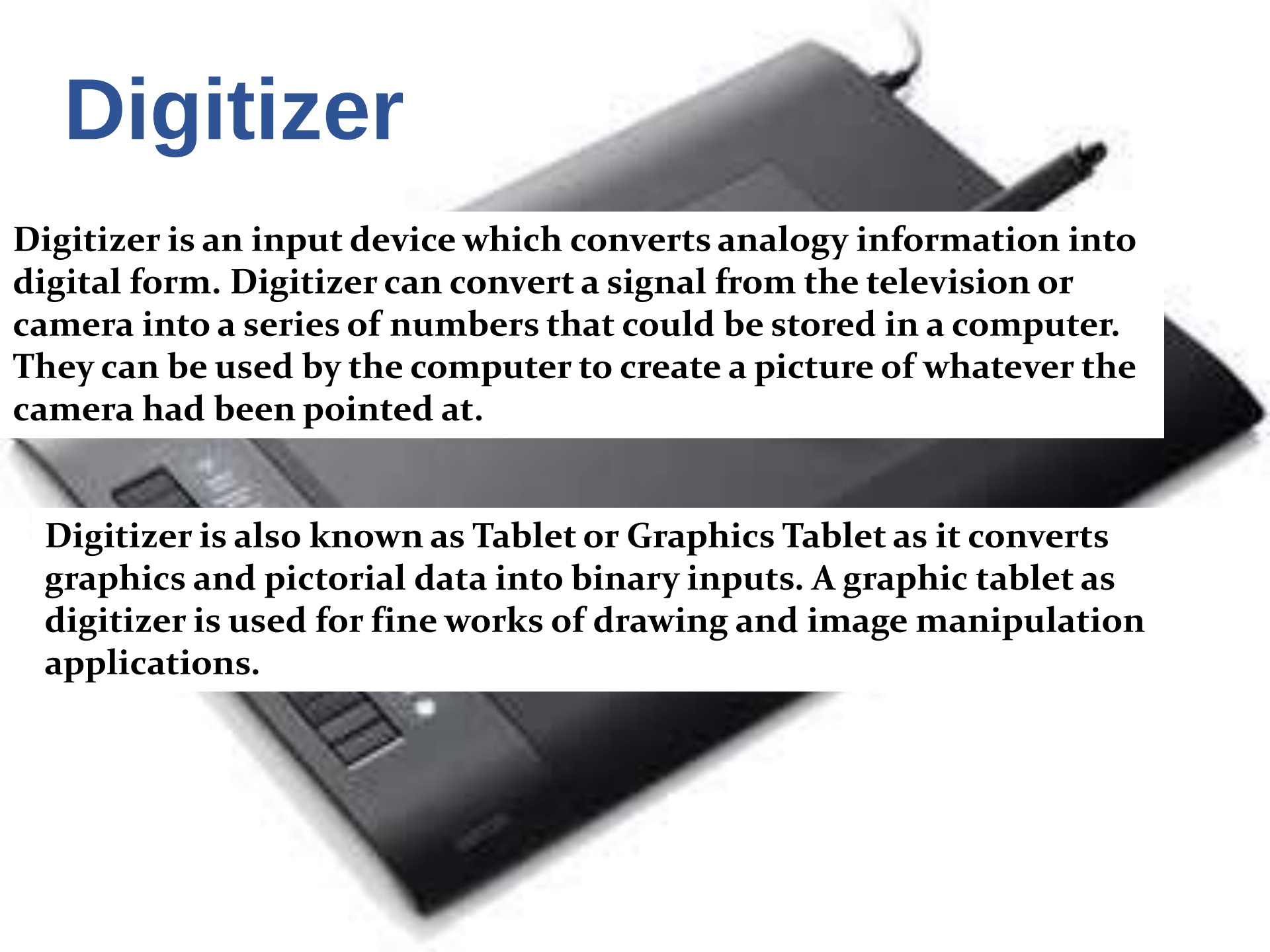
- Track ball is an input device that is mostly used in notebook or laptop computer, instead of a mouse. This is a ball which is half inserted and by moving fingers on the ball, the pointer can be moved.
- Since the whole device is not moved, a track ball requires less space than a mouse. A track ball comes in various shapes like a ball, a button, or a square.

Scanner



- Scanner is an input device, which works more like a photocopy machine. It is used when some information is available on paper and it is to be transferred to the hard disk of the computer for further manipulation.
- Scanner captures images from the source which are then converted into a digital form that can be stored on the disk. These images can be edited before they are printed.

Digitizer



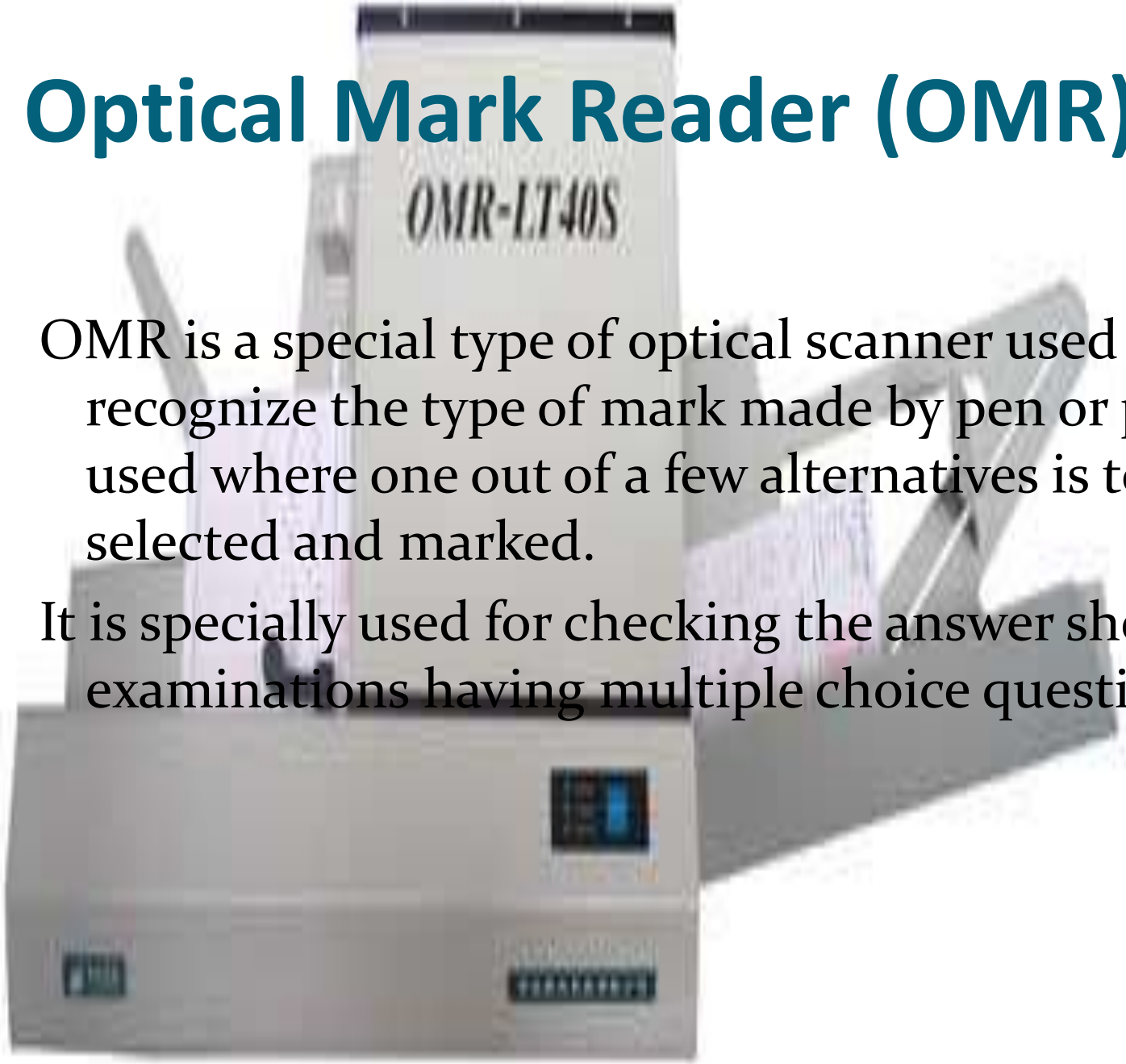
Digitizer is an input device which converts analogy information into digital form. Digitizer can convert a signal from the television or camera into a series of numbers that could be stored in a computer. They can be used by the computer to create a picture of whatever the camera had been pointed at.

Digitizer is also known as Tablet or Graphics Tablet as it converts graphics and pictorial data into binary inputs. A graphic tablet as digitizer is used for fine works of drawing and image manipulation applications.

Bar Code Readers

- Bar Code Reader is a device used for reading bar coded data (data in the form of light and dark lines). Bar coded data is generally used in labelling goods, numbering the books, etc. It may be a handheld scanner or may be embedded in a stationary scanner.
- Bar Code Reader scans a bar code image, converts it into an alphanumeric value, which is then fed to the computer that the bar code reader is connected to.

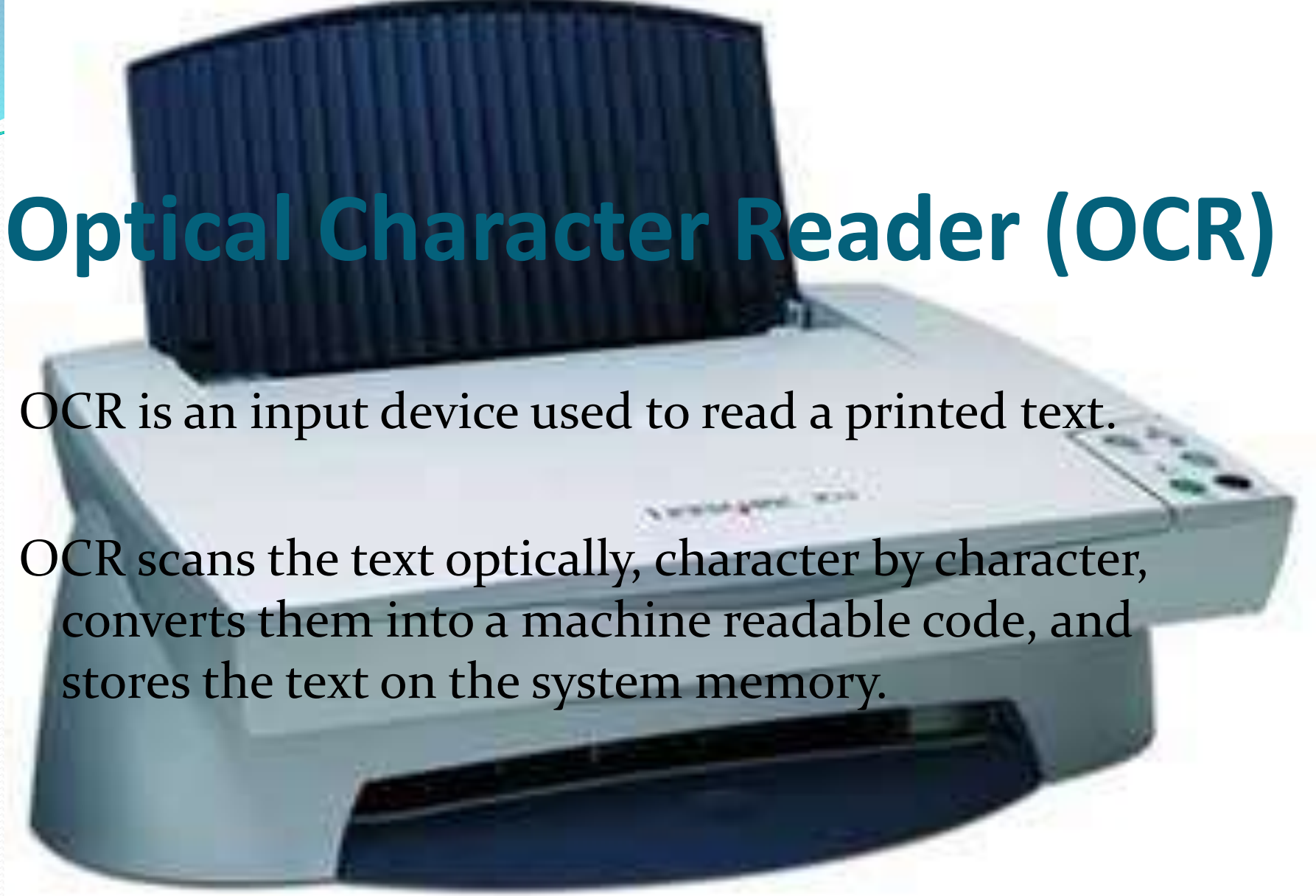
Optical Mark Reader (OMR)



OMR is a special type of optical scanner used to recognize the type of mark made by pen or pencil. It is used where one out of a few alternatives is to be selected and marked.

It is specially used for checking the answer sheets of examinations having multiple choice questions.

Optical Character Reader (OCR)

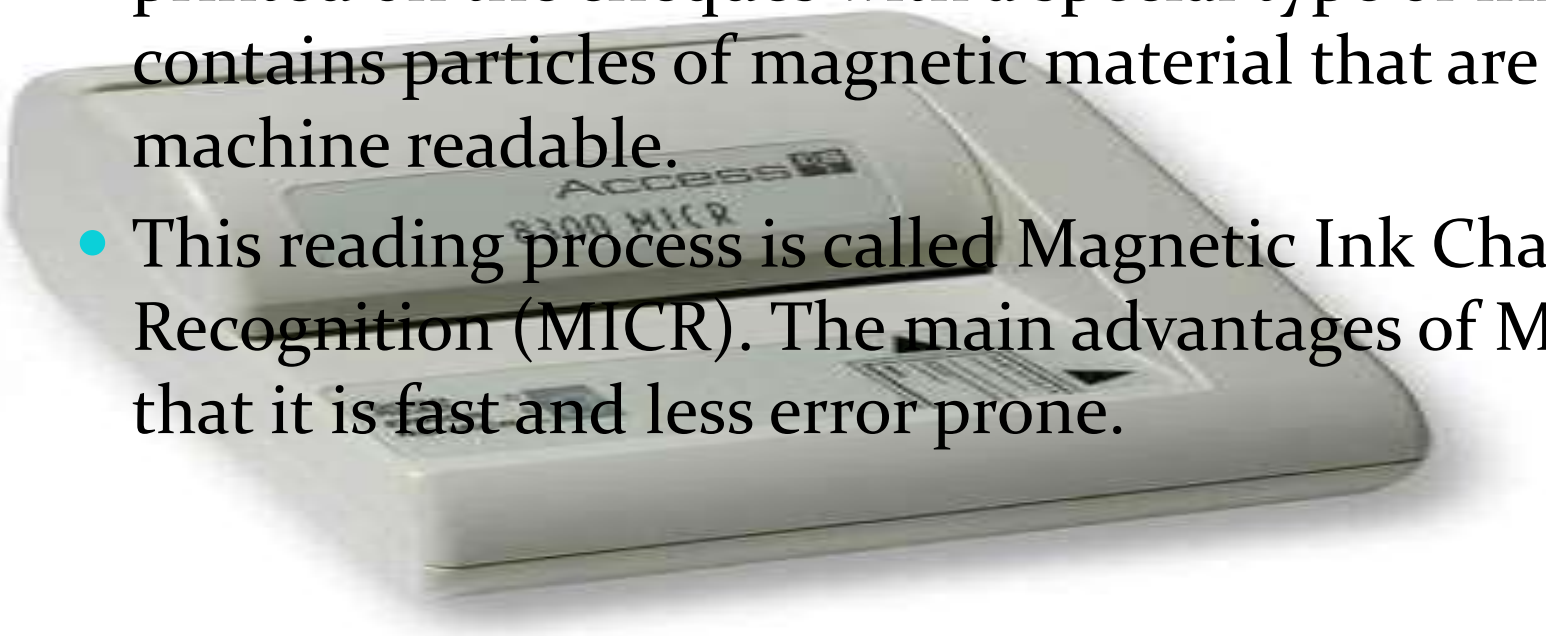


OCR is an input device used to read a printed text.

OCR scans the text optically, character by character, converts them into a machine readable code, and stores the text on the system memory.

Magnetic Ink Card Reader (MICR)

- MICR input device is generally used in banks as there are large number of cheques to be processed every day. The bank's code number and cheque number are printed on the cheques with a special type of ink that contains particles of magnetic material that are machine readable.
- This reading process is called Magnetic Ink Character Recognition (MICR). The main advantages of MICR is that it is fast and less error prone.



Microphone

- Microphone is an input device to input sound that is then stored in a digital form.
- The microphone is used for various applications such as adding sound to a multimedia presentation or for mixing music.

- **Microphone** – an input device that allows users to input audio into their computers. Here are some uses of the microphone:
  - Audio for video
  - Computer gaming
  - Online chatting
  - Recording musical instruments
  - Recording voice for dictation, singing and podcasts
  - Voice recorder
  - Voice recognition
  - VoIP – Voice over Internet Protocol


THANK YOU!

INTERNET OF THINGS

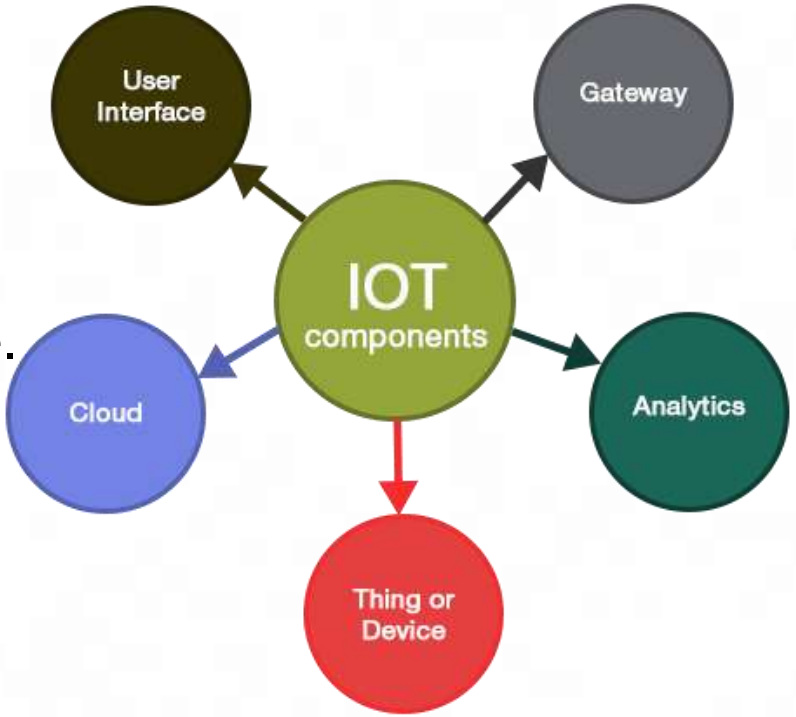
Mrs. A. KALAISELVI
Assistant Professor,
Department of computer Science,
Arul Anandar college Karumathur.

What Is IOT:

- The **Internet of Things** (IoT) refers to the network of physical objects or "things" that are embedded with sensors, software, and other technologies to collect and exchange data with other connected devices and systems over the internet.

- These objects can range from everyday household items like refrigerators and thermostats to industrial machines, vehicles, and even wearable devices.

Key components of IoT



1. **Sensors and Actuators:**

Sensors: Devices equipped with sensors can measure various parameters such as temperature, humidity, motion, light, and more.
Actuators: These devices can perform actions based on the data received from sensors. For example, actuators can control motors, switches, or valves based on sensor data.

2. **Connectivity:**

Internet Connectivity: IoT devices are connected to the internet, allowing them to send and receive data. This connection can be wired or wireless and utilizes various communication protocols like Wi-Fi, Bluetooth, cellular networks, LoRaWAN, etc.

3. Data Processing and Analysis:

- **Edge Computing:** Some IoT devices process data locally (at the edge of the network) rather than sending all data to a centralized server. Edge computing reduces latency and bandwidth usage.
- **Cloud Computing:** IoT data is often sent to cloud servers for storage, analysis, and generating insights. Cloud platforms provide computational power and storage necessary for handling large volumes of data.

4. User Interface:

- **Applications and Dashboards:** IoT data can be visualized through web or mobile applications. Users can monitor and control IoT devices remotely through these interfaces.
- **Voice and AI Interfaces:** IoT devices are increasingly integrated with voice assistants and AI technologies, allowing users to interact with them using natural language commands.

5. Security and Privacy:

- **Encryption:** IoT data transmission is often encrypted to ensure data privacy and security.
- **Authentication and Authorization:** Devices and users need to be authenticated and authorized to access IoT systems and data.
- **Firmware and Software Security:** Ensuring that IoT devices are protected against hacking attempts, including regular security updates.

Control Neighbourhood

1. Localized Control:

- Devices within a control neighborhood can communicate with each other directly or through a local gateway. This localized communication enables faster response times and reduced dependency on external networks, enhancing efficiency and reliability.

2. Real-time Decision Making:

- Devices in a control neighborhood can process data and make real-time decisions without relying on centralized servers or cloud-based systems. This is particularly important for applications where instant responses are critical, such as industrial automation or smart home security.

3. Collaborative Operation:

- Devices in a control neighborhood can work collaboratively, sharing data and insights to optimize their operation. For example, in a smart home, sensors in different rooms might collaborate to regulate temperature and lighting based on occupancy and preferences.

4. Security and Privacy:

- Control neighborhoods can implement localized security protocols, ensuring that communication within the network is secure and devices are protected from unauthorized access. Additionally, data processing within a local network can enhance privacy by minimizing the need to transmit sensitive information over external networks.

5. Scalability and Interoperability:

- Control neighborhoods can be designed to be scalable, allowing easy addition of new devices. Interoperability standards and protocols ensure that devices from different manufacturers can work together seamlessly within the neighborhood.

6. Use Cases:

- Control neighborhoods are applicable in various scenarios, including smart homes, industrial automation, smart cities, agriculture, healthcare, and more. In industrial settings, for instance, a control neighborhood could comprise interconnected sensors, actuators, and machines working together to optimize manufacturing processes.

Challenges and Considerations:

- **Reliability:** Ensuring that devices within the neighborhood can operate reliably and autonomously.
- **Data Management:** Efficient handling and processing of data within the local network.
- **Energy Efficiency:** Optimizing the energy consumption of IoT devices to prolong their operational life.
- **Maintenance:** Regular maintenance and updates to ensure the smooth operation of devices.
- **Security:** Implementing robust security measures to protect against cyber threats and unauthorized access.

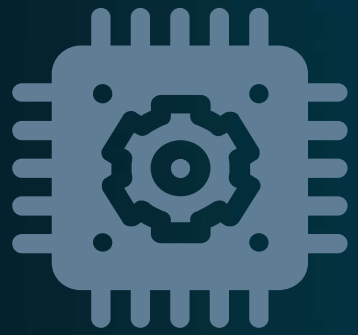
Control Area works in IoT:

1. **Device Integration**: IoT devices within a Control Area are integrated into a network, enabling them to communicate with each other and with a central control system.

2. **Data Collection:** Sensors within the Control Area collect data from the environment. This data could include temperature, humidity, light levels, motion, or any other relevant information depending on the application.

3. **Data Processing:** The collected data is processed locally within the Control Area. This processing might involve filtering, aggregation, or other forms of analysis to extract meaningful information from raw sensor data.

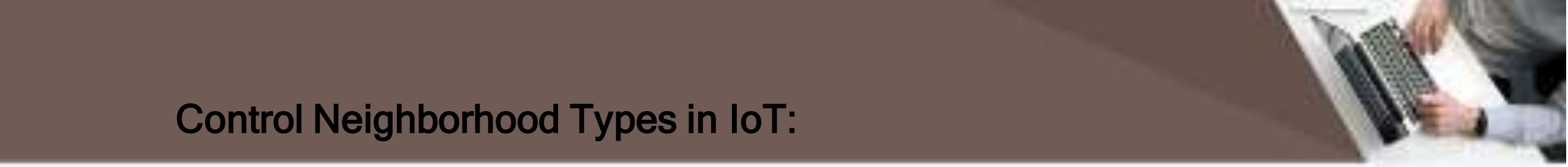
4. **Decision Making:** Based on the processed data, decisions are made within the Control Area. These decisions could be simple threshold-based rules (e.g., if temperature exceeds a certain value, activate the cooling system) or more complex algorithms that analyze multiple data points to make decisions.



1. **Actuation:** Once decisions are made, commands are sent to actuators within the Control Area. Actuators are devices that perform actions based on received commands. For example, a valve could be opened or closed, a motor could be activated, or an alarm could be triggered.

2. **Monitoring and Optimization:** The Control Area continuously monitors the status and performance of IoT devices. This information is used to optimize operations, improve efficiency, and ensure that devices are functioning correctly.

3. **Communication:** The Control Area may also communicate with higher-level control systems or other Control Areas in larger IoT deployments. This communication allows for coordination between different parts of the IoT network.



Control Neighborhood Types in IoT:

- a control neighborhood refers to a network architecture that facilitates the communication and coordination among IoT devices within a specific area.

- Control neighborhood types are classifications used to describe how IoT devices are organized and controlled within a particular environment.

There are several control neighborhood types in IoT:

1. Centralized Control Neighborhood:

- In a centralized control neighborhood, all IoT devices communicate with and are controlled by a central entity, such as a server or a gateway device.

- This central controller manages the communication, data processing, and decision-making for all devices within the network. This type of architecture offers a high level of control and coordination but can be a single point of failure.

2. Distributed Control Neighborhood:

- In a distributed control neighborhood, the control and decision-making processes are distributed across multiple devices within the network.
- Each device has a certain level of autonomy and can communicate and make decisions locally.
- Devices can collaborate with each other without relying on a central controller.
- This architecture provides better fault tolerance and scalability compared to centralized control.

3. Hierarchical Control Neighborhood:

- Hierarchical control neighborhoods have multiple levels of control within the network.
- Devices are organized in a hierarchical structure, where lower-level devices report to higher-level controllers, forming a tree-like topology.
- Each level of the hierarchy has its own set of responsibilities and control functions.
- This type of architecture is useful for managing large-scale IoT deployments efficiently.

4. Mesh Control Neighborhood:

- Mesh control neighborhoods consist of devices that can communicate with each other directly, forming a mesh network.
- Each device in the network acts as a relay, passing data to other devices within the mesh.
- Mesh control neighborhoods are self-organizing and offer high reliability and fault tolerance.
- They are particularly useful in scenarios where devices are spread out over a wide area and need to communicate with each other without relying on a central point of control.

5. Cluster-Based Control Neighborhood:

- In a cluster-based control neighborhood, devices are grouped into clusters, and each cluster has a cluster head that coordinates the communication within the cluster.
- Cluster heads can communicate with each other or with a central controller, enabling efficient communication and management within the clusters.
- This approach is useful for balancing the load and managing network traffic in large IoT deployments.


Thank You