Machine Learning Algorithms for Medical Images Security

Supervised by: Dr.Bashar M. Nema

Prepare by: Noor T. Mahmood and Wrood H. Khalil

Outline

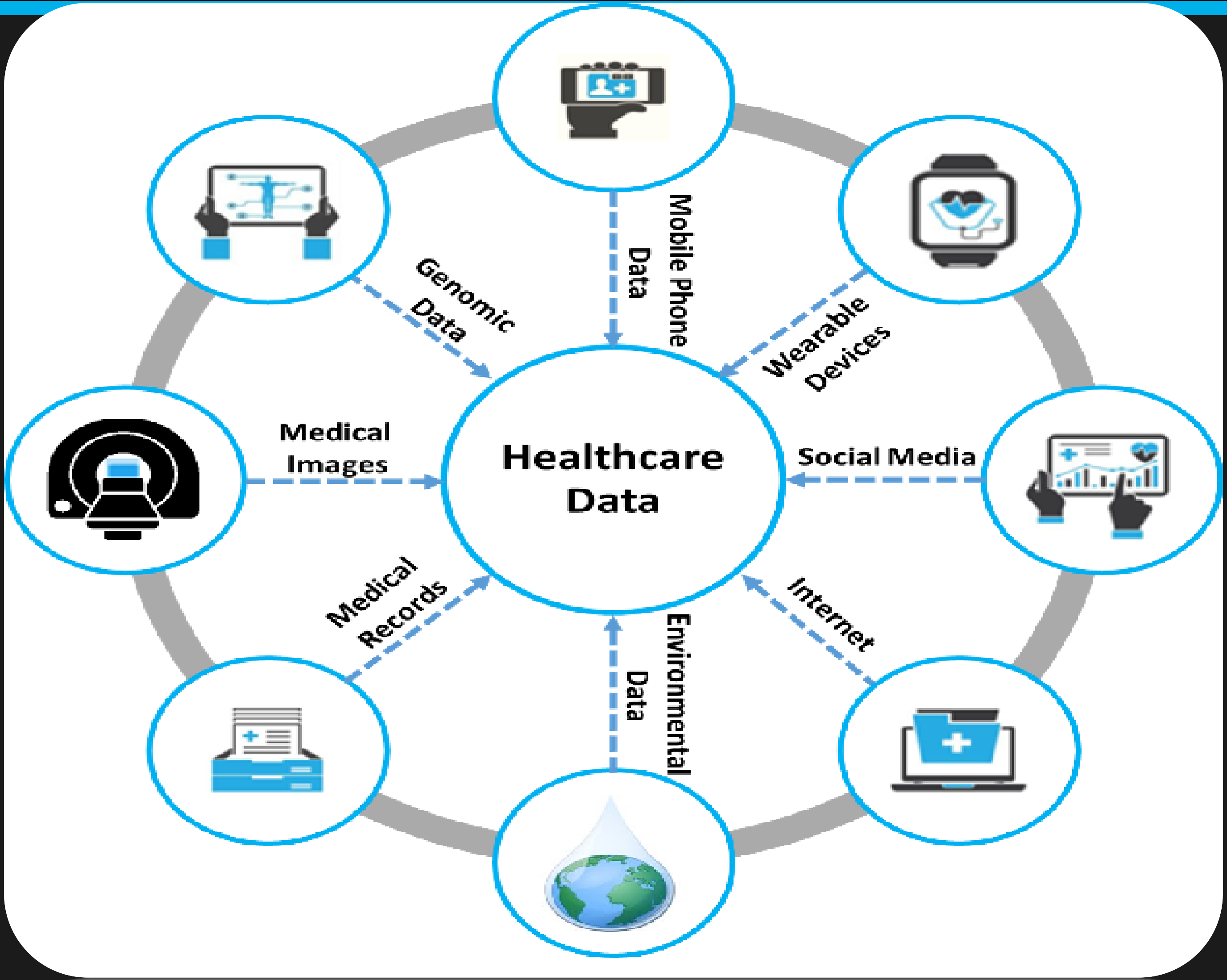
- Abstract
- Introduction
- Background Theory
  - ✓ Machine Learning (ML)
  - ✓ Deep Learning (DL)
  - ✓ Convolution Neural Networks (CNNs)
  - ✓ Medical Image Encryption
  - ✓ Medical Image Steganography
- Review of Different ML Models
- Conclusion
- Reference

Abstract

A high level of safety and security is required for medical image transmission via open access since medical pictures are more important than other images in most applications, especially in real-time applications like telemedicine. Unique characteristics in many imaging data make it difficult to analyze and decide on the techniques needed to protect confidential images from unauthenticated access. Current encryption techniques primarily target textual data; they do not, however, work well with multimedia data, such as photos. Even though telemedicine is a medical business, the medical community opposes data computing because it violates the confidentiality and validity of medical data because of the ease with which informatics makes it possible to do so.

Several research projects are discussed in this paper from a confidentiality standpoint in medical aid, which uses these technologies and has related challenges: The use of machine learning (ML) for safe healthcare The overview of the review article summarizes the findings of several experiments and shows that they are quick, effective, secure, and retain optimal performance.

Healthcare service providers generate a large amount of Heterogeneous data and information

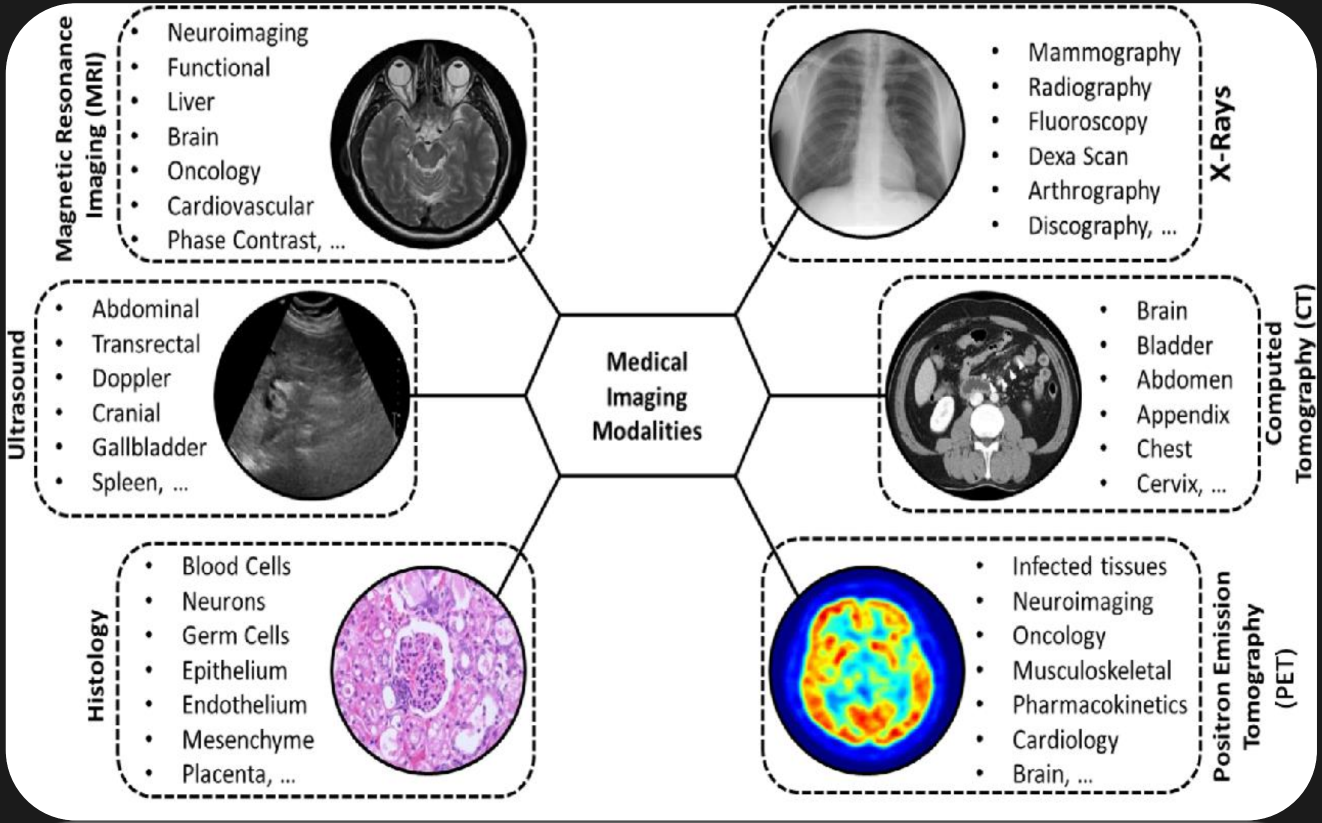


Introduction

- Medical images are crucial and sensitive data in medical computer systems [1]. Medical images are transmitted over an insecure internet connection; a consistent encryption system is devised. Among the three basic qualities of the Central Intelligence Agency (CIA) (Confidentiality, Integrity, and Availability), the important characteristic of the communication of medical pictures between doctors is secrecy [2].
- With the fast expansion of electrical information interchange, it is vital to secure the privacy of picture data from unwanted access [3].
- Defilements of security can affect the confidentiality and reputation of users.
- Therefore, data encryption is commonly used in open networks such as the internet to ensure safety [4].
- Digital picture security has grown in popularity as a result of the huge rise in digital data transfer over public channels.
- It garners an overwhelming amount of attention in today's digital age. Throughout our society, advancements in multimedia technology have enabled digital images to take on a greater role than traditional papers, which require extensive confidentiality protection for all uses.
- Because each data format has distinct benefits, distinct measures must be utilized to safeguard sensitive picture data from unauthorized access [5].

Introduction (con.)

- There is an interdisciplinary field known as the Internet of Medical Things, which applies Internet-of-Things technology to the field of medicine Medical imaging (brain "Magnetic Resonance Imaging (MRI)" for cancer diagnosis and "Computed Tomography (CT)") of the lung for nodule identification) has benefited from the development of IoMT [9]-[11].



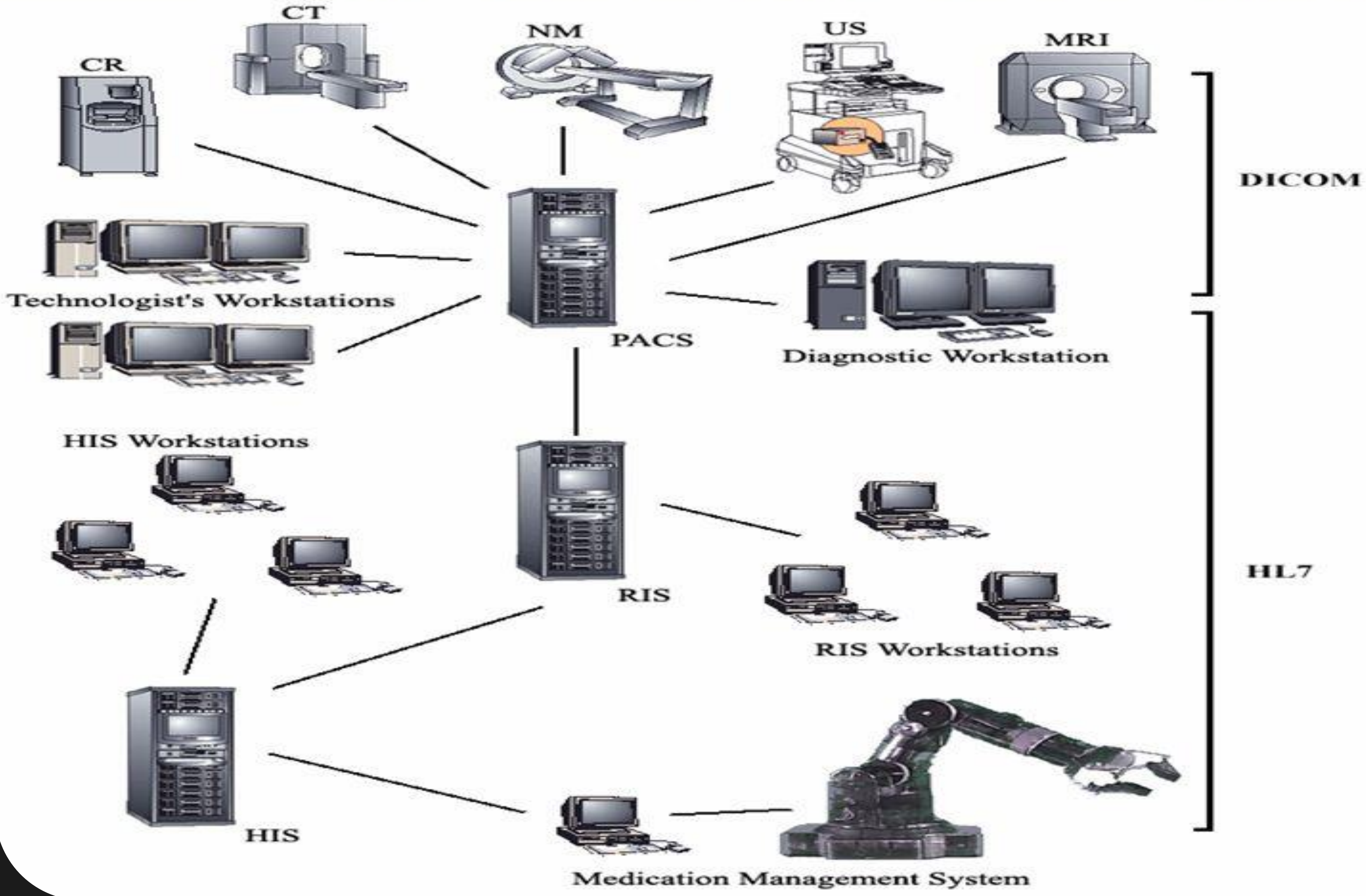
Introduction (con.)

- Archiving and sharing of medical pictures is commonly done using Picture Archiving and Communication Systems (PACS) [12] The equipment is extensively networked and is used to aid doctors in diagnosing and treating patients, e.g. Therapeutic images are frequently supervised in IoMT by a system called Picture Documentation and Communication Systems.

- When therapeutic imaging equipment detects a silent, it stores it in the PACS.

- If an adversary, either internal or external, gains access to the Hospital Information System (HIS)or Archiving and Communication Systems (PACS), it becomes trivial to eavesdrop on these medical pictures, resulting in a significant breach of patient privacy [12].

Typical Hospital IT Systems

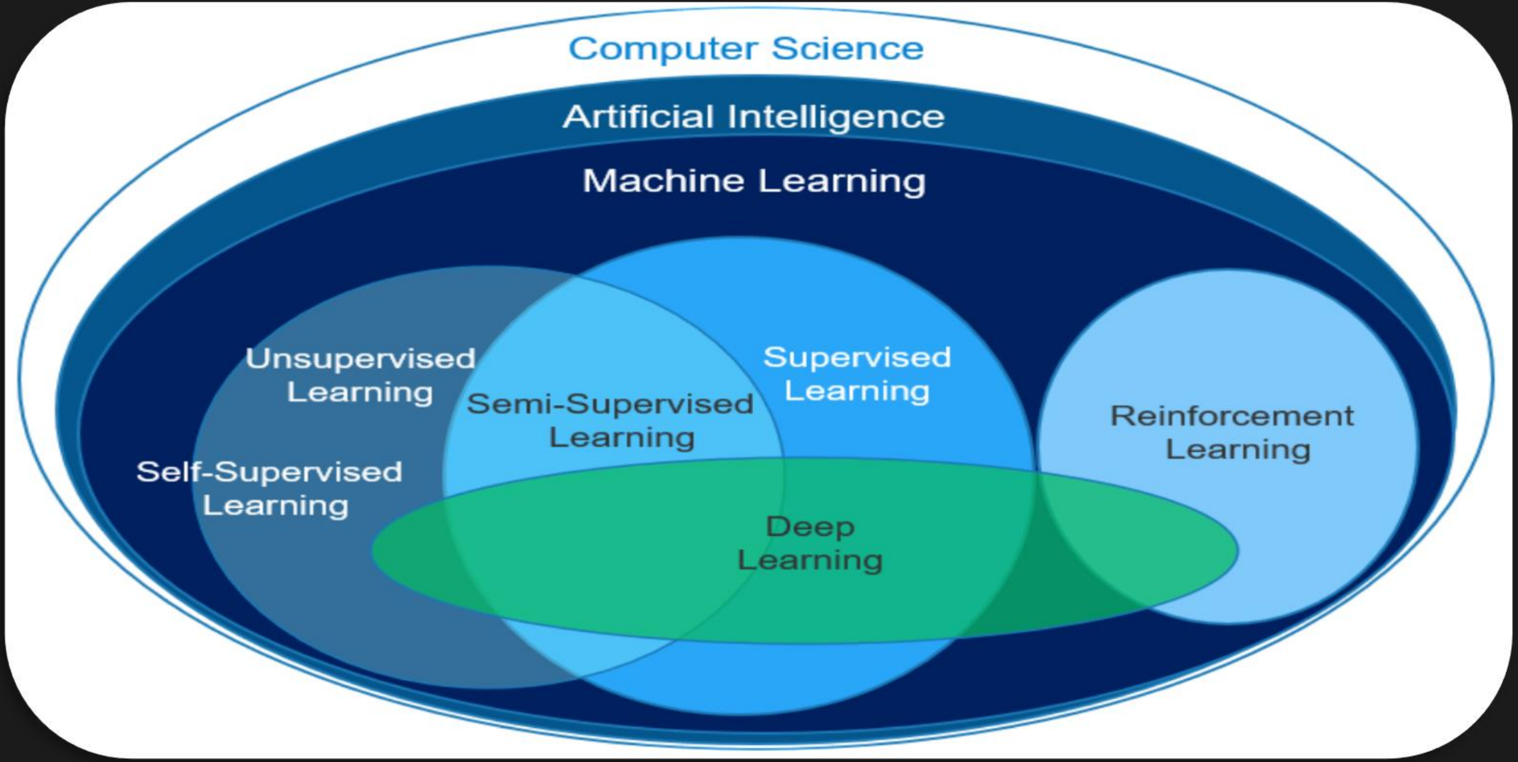


Interactions among hospital IT systems including modalities, picture archiving and communications system (PACS), radiology information system (RIS), hospital information system (HIS), and automation systems

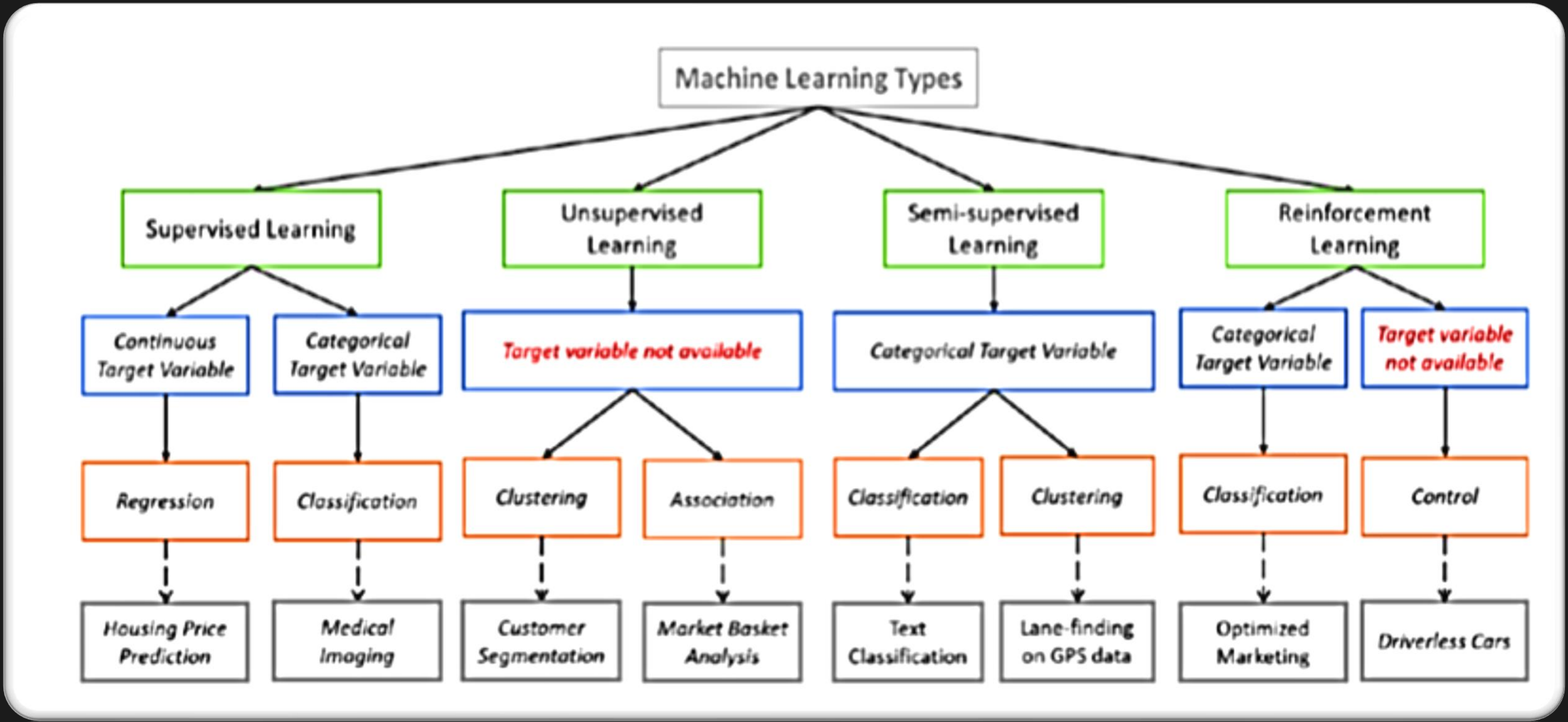
Background Theory: Machine Learning (ML)

AI and ML have gained prominence in recent years, notably in medicine, where they are used in fields such as computer-assisted diagnostic and surgical procedures, medical image interpretation, and image analysis. These methods can assist physicians in precisely diagnosing and anticipating disease, therefore mitigating or avoiding disease's impact.

The primary difference between predictable techniques and ML is that ML is based on inputs and outputs rather than rules. The inputs are the extracted characteristics from the application, and the productions are the labels. ML algorithms establish a broad model by mapping inputs to outputs



Types Machine Learning



Machine Learning Types

Supervised Learning

Unsupervised Learning

Semi-supervised Learning

Reinforcement Learning

Continuous Target Variable

Categorical Target Variable

Target variable not available

Categorical Target Variable

Categorical Target Variable

Target variable not available

Regression

Classification

Clustering

Association

Classification

Clustering

Classification

Control

Housing Price Prediction

Medical Imaging

Customer Segmentation

Market Basket Analysis

Text Classification

Lane-finding on GPS data

Optimized Marketing

Driverless Cars

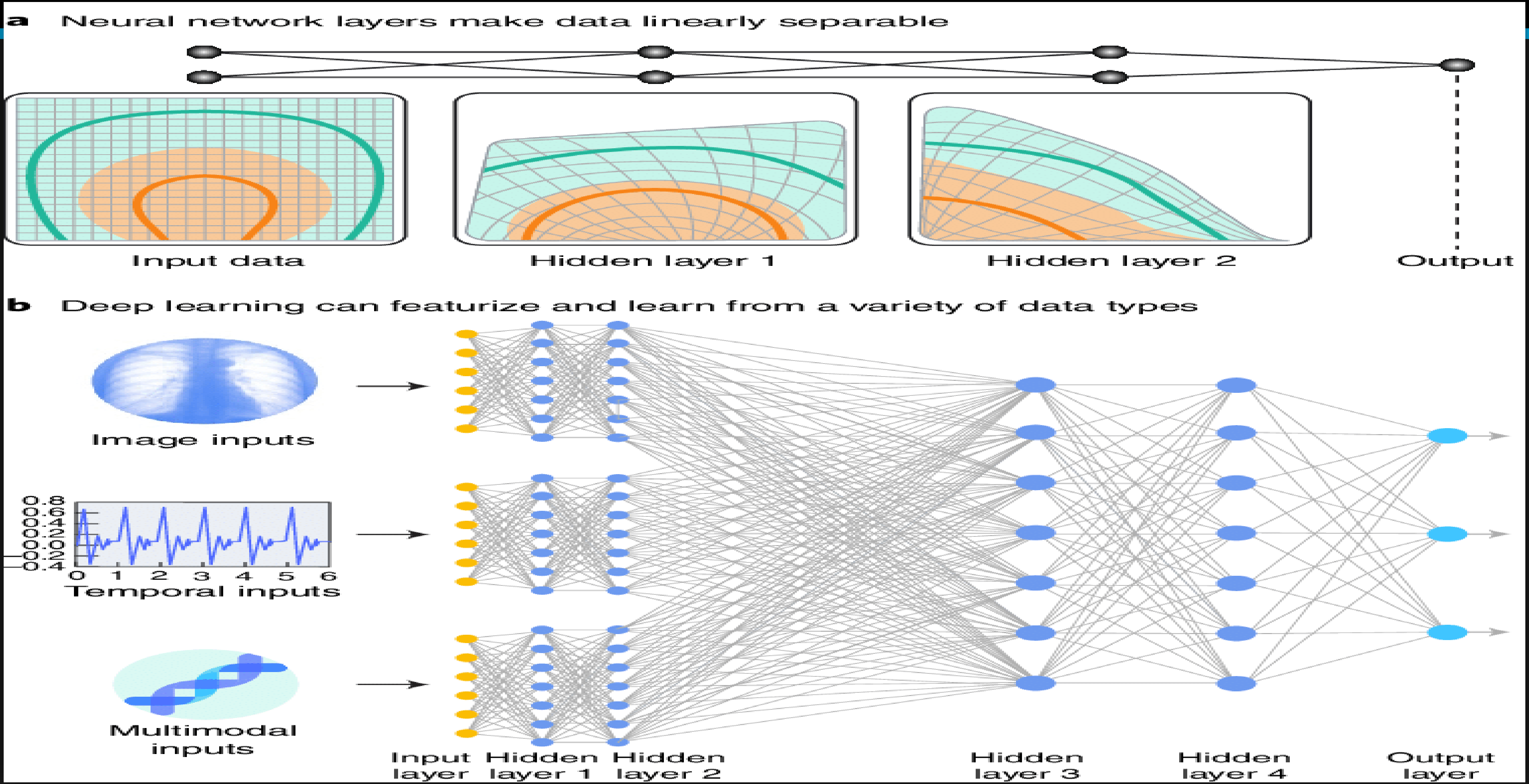
Comparison of different ML models

Learning type	Model building	Examples
Supervised	Models or algorithms get their knowledge from labeled data (Task-driven method)	Classification, regression
Unsupervised	Models or algorithms acquire knowledge from unlabeled data (Data-Driven Method)	Clustering, association, and reduction of dimensionality
Semi-supervised	Models are constructed using a combination of labeled and unlabeled data.	clustering ,Classification
Reinforcement	The models are built on either a reward or a penalty (Environment-driven method)	Classification, control

Background Theory: Deep Learning (DL)

- Typically, ML models are taught to execute certain functions. Practical tasks based on functionality that has been manually extracted from raw data or functionality that has been taught via the use of other rudimentary automated models.
- By skipping this tedious and difficult phase, DL enables computers to automatically discover useful and valuable characteristics directly from data.
- Although several kinds of Artificial Neural Networks (ANN) are the most often used models in education, there are others.
- The primary characteristic that all DL methods have in public is their emphasis on learning functionality: ML of data.
- This is the prime distinction between learning methodologies and more "traditional" machine learning.

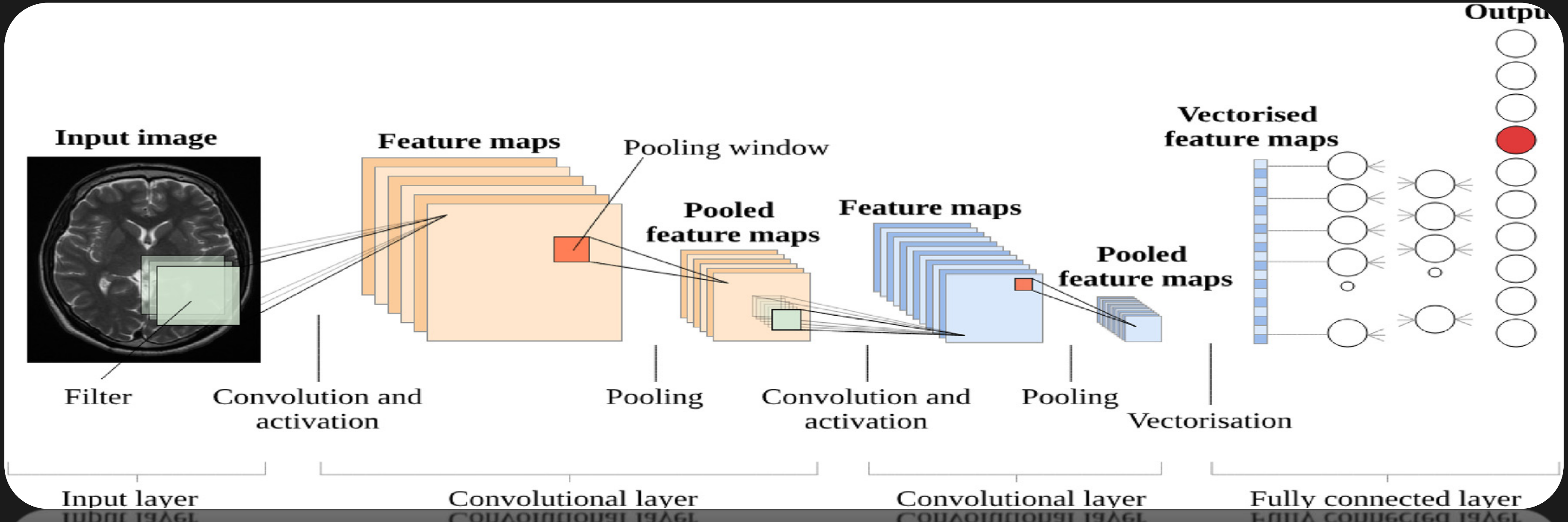
Background Theory: Deep Learning (DL) (con.)



Convolutional Neural Networks (CNNs)

- Convolutional neural networks have sparked interest in DL in medical imaging. A highly effective method for learning advantageous representations of pictures and other designed data. Before CNNs could be used efficiently, characteristic had to be developed by hand or using less capable ML models.

- Once characteristics could be extracted directly from data, numerous hand image features were often omitted. They have been shown to be practically ineffective in comparison to CNN's feature detectors. CNNs are created with strong preferences in mind, which explains why they are so strong. Therefore, let us do a search for the CNN building blocks.



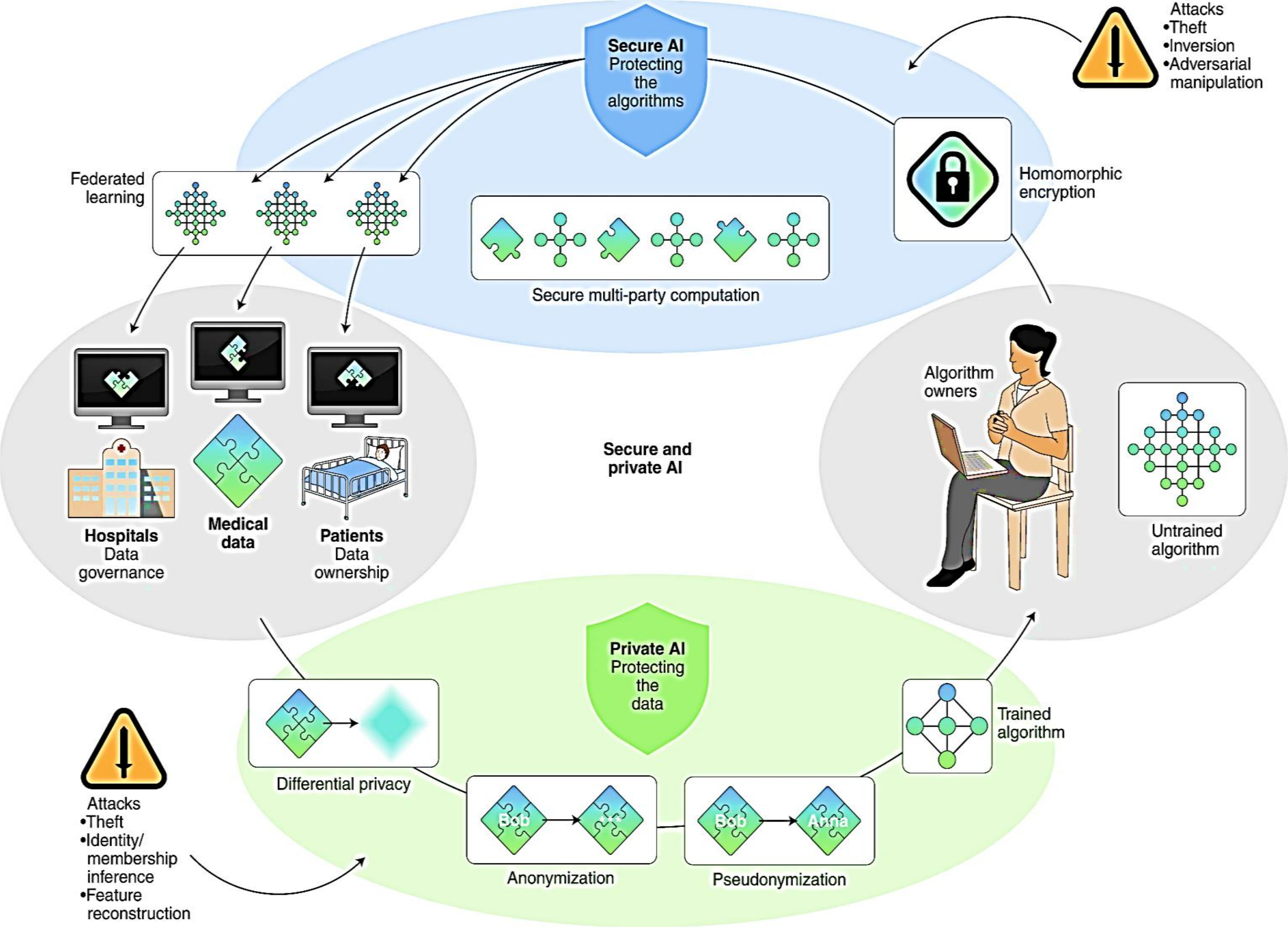
Background Theory: Medical Image Encryption

- To encrypt a image, it is essential to transform the input image to an encryption image using symmetric or asymmetric keys using a symmetric or asymmetric encryption technique.
- Identical codes employ the same key for encryption and decryption, whereas asymmetric codes employ distinct keys for encryption and decryption.
- Encrypting medical images may be accomplished via a variety of algorithms and other factors.
- Encryption of medical pictures is possible using high-speed running, a somewhat smart deployment, chaotic maps, and edge and soon.
- The algorithm performance used to encrypt medical pictures may be determined by looking at the peak noise signal ratio, the bit error rate, the fidelity, and the average square error.
- Encrypting medical images is mostly used for security purposes

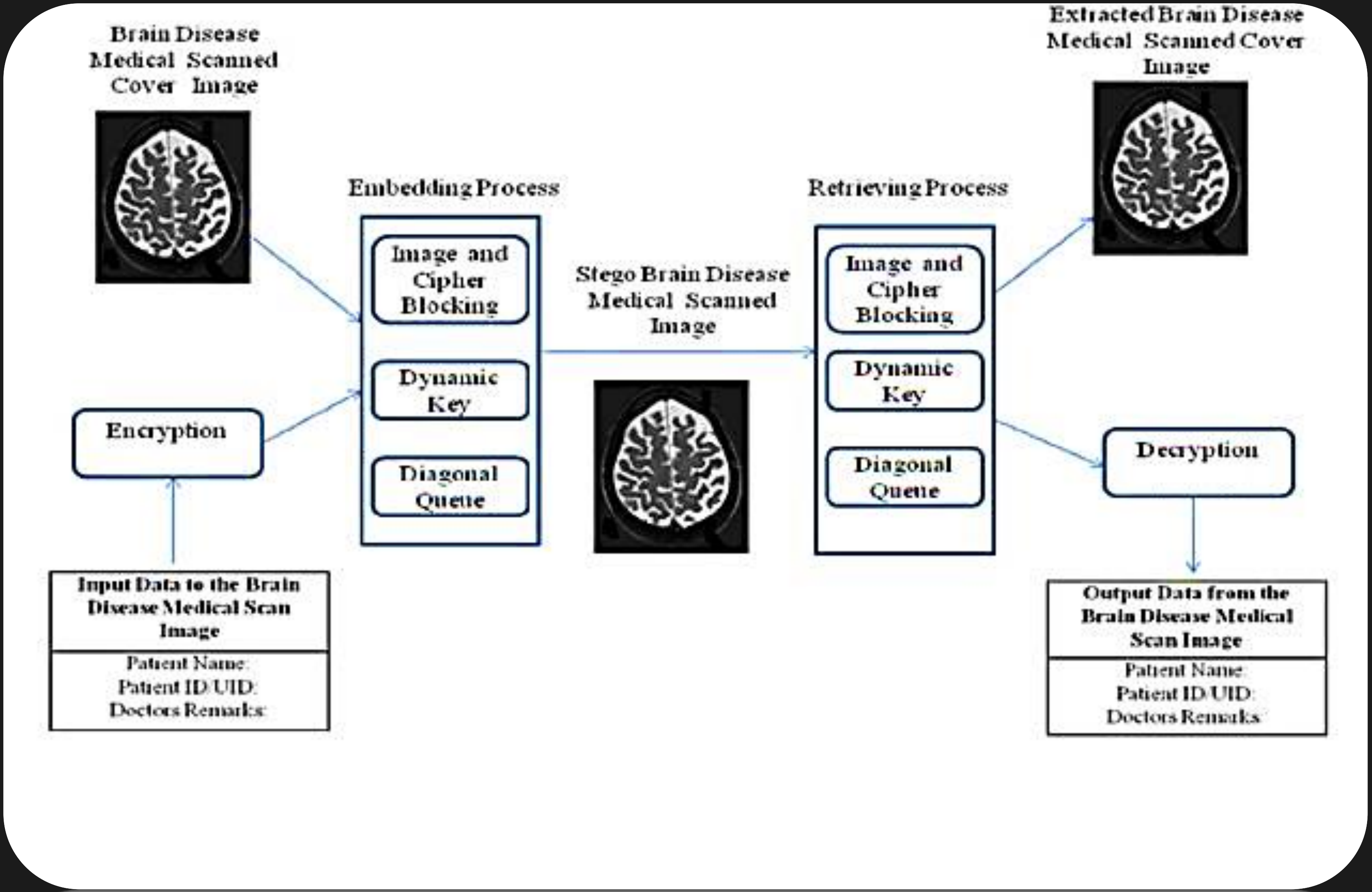
Medical Image Encryption (con.)

Encrypting medical images is mostly used for security purposes.

- ➢ Encrypted transfer of patient medical records
- ➢ Ensuring the confidentiality and integrity of information
- ➢ Avoiding alterations to medical photos that might result in a misleading diagnosis
- ➢ Resist cyberattacks and threats.



Background Theory: Medical Image Steganography


Brain Disease Medical Scanned Cover Image
Embedding Process
Image and Cipher Blocking
Dynamic Key
Diagonal Queue
Encryption
Input Data to the Brain Disease Medical Scan Image
Patient Name:
Patient ID/UID:
Doctors Remarks:
Stego Brain Disease Medical Scanned Image
Retrieving Process
Image and Cipher Blocking
Dynamic Key
Diagonal Queue
Extracted Brain Disease Medical Scanned Cover Image
Decryption
Output Data from the Brain Disease Medical Scan Image
Patient Name:
Patient ID/UID:
Doctors Remarks:

Medical Image Steganography (con.)

The degree of corruption is determined by two factors:

- First, the volume of data to conceal. On a daily basis, it has been used to conceal text messages within photographs. Pixel bits are used to quantify the quantity of concealed data. Frequently, the data size is set to 0.4 or less. The extended the message, the greater the bop, and hence the greater the carrier's alteration.
- Second, the degree of corruption is determined by the carrier image. By concealing information in noisy, frequency-filled portions of a picture, a slight human-visible disturbance is created in flat sections. Estimating the amount of information that an image may conceal can be found in

Models for Secure Medical Image by ML

Review of Different ML Models

Year	Researchers	objective	Data set	Model name	Programming environment	Results	Merits
2018	V. M. Manikandan V. Masilamani	Communication technology advancements and the creation of new medical robotics are extremely beneficial for telemedicine applications.	5000 images from the OsriX dataset were transformed to 8-bit grayscale images with a resolution of 512512 pixels.	Reversible data hiding (RDH)	Matlab2017a was used to develop and test the algorithm on a workstation with 32 GB RAM and an Intel(R) Xeon(R) CPU running at 3.46 GHz.	The suggested structure outperforms previous techniques in terms of mbedding rate and bit error rate on typical medical pictures from the OsriX dataset.	to decrypt the picture with EPR data bits. The suggested structure is unique in that it uses a support vector machine (SVM) based classification structure to extract data and recover images from encrypted images. The suggested structure outperforms the current structures in terms of implanting rate and bit error rate on typical medical pictures from the OsriX dataset.

Review of Different ML Models(Con.)

Year	Researchers	objective	Data set	Model name	Programming environment	Results	Merits
2019	Jin Chao Ahmad Al-Badawi Balagopal Unnikrishnan Jie Lin Chan Fook Mun James M. Brown J. Peter Campbell Michael Chiang JayashreeKalpathy-Cramer Vijay Ramaseshan Chandrasekhar Pavitra Krishnaswamy ,Khin Mi Mi Aung	High performance and resource-efficient implication on high-resolution encryption in practical applications. CaRENets has a novel FHE packaging method with CNN functionalities.	Retinopathy of Prematurity (ROP) grayscale images and DR RGB images	CaRENets	MATLAB 2016a with i5 processor and 4GB RAM.	It enables fast, memory-efficient HE inference without increasing communication strain. This has implications for clinical imaging DLinference.	Memory efficiency (condensed image and CNN activation packing) and inference speed (fewer ciphertexts formed and related math operations) than regular interleaved packing.

Review of Different ML Models(Con.)

Year	Researchers	objective	Data set	Model name	Programming environment	Results	Merits
2019	Weixuan Tang, Bin Li , Shunquan Tan Mauro Barni and Jiwu Huang	Hide a stego message while fooling a stegaanalyzer on a convolutional neural network.	500 thousand JPEG images	convolutional neural network (CNN)-based steganalyzer.	Python interface. The tests were run on an NVIDIA Tesla K80 GPU platform	That opens the door for novel steganographic systems that can overcome sophisticated CNN-based stegaanalysis.	Approach to the steganographic challenge, particularly how to implant the stego message while also opposing a sophisticated CNN-based steganalyzer.
2020	S. J. Sheela K. V. Suresh Deepaknath Tandur A. Sanjay	augment the security of the diffusion operation is employed.	X-rays, magnetic Resonance imaging(MRI) computerized tomography (CT)	CNN-CCT	MATLAB 2009on1.88 GHz Intel CPU with 2.99 GB RAM in Windows XP Professional operating system.	Assume the The suggested cryptosystem is resistant to numerous cryptographic attacks and comparable to current encryption systems.	Highly sensitive to text. So the cryptosystem is safe. The cryptosystem took 121.842689 s to encrypt and decode the medical picture 256,256. The suggested cryptosystem is slower than decryption.

Review of Different ML Models(Con.)

Year	Researchers	objective	Data set	Model name	Programming environment	Results	Merits
2020	Yi Ding, Guozheng Wu, Dajiang Chen, Ning Zhang, Linpeng Gong, Mingsheng Cao, and Zhiguang Qin,	For the privacy-protected environment, a ROI data mining network extracts the intriguing item straight from the encrypted image.	chest Xray dataset	DLEDNet	ROI-mining-network, Processor Nvidia GTX 2080Ti	The findings reveal that the author's approach can encrypt/decrypt medical images more efficiently than other sophisticated medical image encryption methods.	The encryption template keyspace can be 2757936, making it difficult for an adversary to crack. Nevertheless, the iterations and broadcasts private key is difficult. Thus, ciphertext-only assaults are difficult to decipher.
2021	Hokuto Hirano, Akinori Minagi and Kazuhiro Takemoto	Improve knowledge of DNN security issues and assist improve DNN security.	Three medical images: skin lesion images for skin cancer diagnosis, OCT images for diabetic retinopathy diagnosis, and chest images for pneumonia diagnosis.	DNN	Adversarial Robustness Toolbox v1.0.0 universal adversarial perturbation (UAP)	The virtually intangible UAPs won >80% of nontargeted attacks. The UAPs' impotence was based on the exhibited design.	These findings help us better understand DNN adversarial attacks and maybe improve DNN security. UAPs help develop the DNN strategy's dependability.

Conclusion

- The main presentation objective is to discuss methods for safeguarding patient data. The study's primary objective is to increase the security of medical photographs through the use of multiple optimization methods.
- In ML and deep learning, the algorithm model presupposes that a new technique of protection may be implemented more effectively and with little latency than existing approaches. Nevertheless, it achieves a high level of image security and will obtain them without engaging in criminal activity. The findings from each study will demonstrate that the author's suggested sharing strategy ensures the image's secrecy, integrity, and dependability.
- The performance study of all approaches in this article demonstrates the security, efficacy, and resilience of the author's suggested algorithm. T
- his article contributes to ongoing research in the arena of medical image processing and security.

- By utilizing sophisticated machine learning techniques in artificial intelligence (AI), we propose that work be done to reduce the processing time for encoding CT SCAN pictures in order to fulfill real-time communication needs. It may suggest a novel way for securely transmitting COVID-19 CT pictures in the real world.

Thank you for Listening!