Cryptography and Network Security

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages, various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include military communications, electronic commerce, ATM cards, computer passwords and many more.

Modern cryptography is heavily based on mathematical theory and computer science practice cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power an example is the one-time pad but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

Network security refers to any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Image & Video Processing

The course deals with Concepts and application in image and video processing. Which will provide a mathematical framework to describe and analyze images as two-dimensional(2D) signals in the spatial, temporal, and frequency domains. Two-dimensional sampling and quantization are studied, and the human visual system is reviewed. Various transforms to modify and extract information from image. The course will cover techniques and tools for image processing, and introduce image analysis techniques in the form of image segmentation, restoration/degradation model.

Video signal processing address how to efficiently represent multimedia data, including video, image, audio and text and how to deliver them over a variety of networks. In the coding aspect, state-of-the-art compression technologies will be presented. Emphasis will be given to a number of standards, including H.26x, Moving Picture Expert Group (MPEG), and Joint Photographic Expert Group (JPEG).

Applications are discussed in frame interpolation, filtering, coding, noise suppression, and video compression. The course is primarily meant to develop on-hand experience in applying these tools to process images and video. With fundamentals of Image & Video Processing, learners can explore applications, computer vision and machine learning, machine perception, medical imaging, human pose estimation, learning to count an objects in image/video, data compression, augmented and virtual reality, pattern classification and identification etc.,

Power Electronics

Power electronics is the application of solid-state electronics to the control and conversion of electric power. It also refers to a subject of research in electronic and electrical engineering which deals with the design, control, computation and integration of nonlinear, time-varying energy-processing electronic systems with fast dynamics. The first high power electronic devices were mercury-arc valves. In modern systems, the conversion is performed with semiconductor switching devices such as diodes, transistors and thyristors, pioneered by R. D. Middlebrook.

Some discrete components used in power electronics: Power Diodes, Schottky Diodes, Power Bipolar Junction Transistors, Power MOSFETs, Thyristors ,Silicon Controlled Rectifier (SCR), Gate Turn-Off Thyristors, Insulated Gate Bipolar Transistors (IGBT), Gate-Commutated Thyristors

In contrast to electronic systems concerned with transmission and processing of signals and data, in power electronics substantial amount of electrical energy is processed. AC/DC converter (rectifier) is the most typical power electronic device found in many consumer electronic appliances, e.g. television sets, personal computers, battery chargers, etc. The power range is typically from tens of watts to several hundred watts. In industry, a common application

is the variable speed drive (VSD) that is used to control an induction motor. The power range of VSDs start from a few hundred watts to tens of megawatts.
The power conversion systems can be classified according to the type of the input and output power, AC to DC (rectifier),DC to AC (inverter), DC to DC (chopper),AC to AC (controller).The capabilities and economy of power electronic systems are determined by the active devices that are available. Power electronic devices may be used as switches, or as amplifiers.

Soft Computing

In computer science, soft computing (referred as computational intelligence) is the use of inexact solutions to computationally hard tasks such as the solution of Nondeterministic Polynomial time complete problems, for which there is no known algorithm that can compute an exact solution in polynomial time. Soft computing differs from conventional (hard) computing in that, unlike hard computing, it is tolerant of imprecision, uncertainty, partial truth, and approximation. In effect, the role model for soft computing is the human mind.

Soft Computing became a formal area of study in Computer Science in the early 1990s. The soft computing solutions are unpredictable, uncertain, Earlier computational approaches could model and precisely analyze only relatively simple systems. More complex systems arising in biology, medicine, the humanities, management sciences, and similar fields often remained intractable to conventional mathematical and analytical methods. However, it should be pointed out that simplicity and complexity of systems are relative, and many conventional mathematical models have been both challenging and very productive. Soft computing deals with imprecision, uncertainty, partial truth, and approximation to achieve practicability, robustness and low solution cost. As such it forms the basis of a considerable amount of machine learning techniques. Recent trends tend to involve evolutionary and swarm intelligence based algorithms and bio-inspired computation.

Components of soft computing include:

- Machine learning, including:
    - Neural networks (NN)
        - Perceptron
    - Support Vector Machines (SVM)
- Fuzzy logic (FL)
- Evolutionary computation (EC), including:
    - Evolutionary algorithms
        - Genetic algorithms
        - Differential evolution
    - Metaheuristic and Swarm Intelligence
        - Ant colony optimization

        - Particle swarm optimization
- Ideas about probability including:
    - Bayesian network

Soft computing techniques resemble biological processes more closely than traditional techniques, which are largely based on formal logical systems, such as predicate logic, or rely heavily on computer-aided numerical analysis.