**1.1 INTRODUCTION TO IMAGES**

An image consisting of data (specifically a set of elements) defined on an n-dimensional regular grid that has the potential for display. These elements are referred to as pixels. Pixels in different images ay represent a variety of information, such as temperature, pressure, velocity, terrain height, or tissue density. The regular grid is frequently over two-dimensional space but can be three-dimensional, and four- dimensional if sampling over tie is also included.

**1.1.1 Digital Image:** A digital image can be considered as a function F(x,y), where (x,y) represents the co-ordinate position of the pixel and F represents the amplitude of the pixel at position(x,y).

**1.1.2 Gray Scale Image:** A gray scale image is an image where pixel value at any image point can be represented by a single valued function with a range of 0 to 2N-1 for an N-bit image. Here, measurement is done in only one axis i.e. Luinance(1) or Intensity(I) of the pixels.

**1.1.3 Colour image:** Images may be multi-valued also by making more than one measurement at a point, So, for a colour image F(x,y) will be a tuple representing a colour in a colour system. For example any RGB colour image can be represented by the intensity of red, green and blue for each pixel position(x,y).

**1.2 INTRODUCTION TO CRYPTOGRAPHY**

Cryptography is a science of keeping secrets secret. The word cryptography comes from the Greek word "kryptos" meaning "hidden" and "graphein" meaning "to write". The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it.

Assume a sender referred to here as Alice wants to send a message to a receiver referred to as Bob.If anyone send message through the network, if message contains confidential information. The message could be intercepted and read by eavesdropper or, even worse, the adversary might be able to modify that message during transmission in such a way that the legitimate recipient Bob does not detect the manipulation. One objective of cryptography is to provide methods for preventing such attacks.

**1.3 CONTEXT OF CRYPTOGRAPHY**

Cryptology, the study of cryptosystems, can be subdivided into two branches −

* Cryptography
* Cryptanalysis

Cryptology

Cryptanalysis

Cryptography

Figure 1.1: Context of Cryptography

### 1.3.1 Cryptography: Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

### 1.3.2 Cryptanalysis: The art and science of breaking the cipher text is known as cryptanalysis. Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

**1.4 ENCRYPTION AND DECRYPTION**

Encryption is a process that transforms the first information into an unrecognizable form. The process that converts plaintext to cipher form is called encryption. The new form of the message is wholly different from the original message. An original massage is named as the plaintext, while the encoded message is named as cipher-text. The transmission from the cipher-text into plaintext is known as decryption process. This form of message is read and understood by a human or a computer. Many schemes are there that are used for encryption. Such a method is understood as a cryptographic scheme or a cipher. Schemes used for decrypting a message with none knowledge of the encrypted details falls under the world of cryptanalysis. The area of cryptography and cryptanalysis is jointly called cryptology [23].

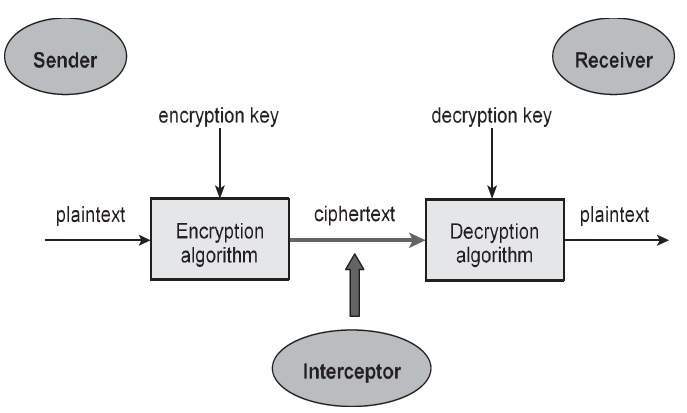


Figure 1.2: The Cryptography Model

**1.5 CRYPTOGRAPHY TECHNIQUES**

The two types of cryptography techniques are given below:

**1.5.1 Symmetric Key or Private key Cryptography:** Symmetric key algorithm is also known as private key cryptography algorithm. This method uses sae keys for both enciphering and deciphering. Examples of Symmetric key encryption are - Blowfish, DES, AES, RC4, RC5, and RC6.