Chapter 3

Medical and Biological Image Analysis

Abdelkader Moumen

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75491

Abstract

Today, technology and information communication are deeply embedded in our life. Information is present and used in many forms: electronic documents, audio, videos, photos, etc. Recent advances in technology, particularly in the computer industry and communication, have motivated organisations to replace their traditional manually stored and exchanged records with computer systems and digital documents for secure storage and smooth transmission. Medical and biological image processing is a numerical method and technique for modifying a digital image to improve or extract information. The main stages of image processing are:

1. acquisition of the image: by cameras, radars, sensors and so on;

2. image enhancement: Highlight some components of the image or reveal details and make the image clear.

3. image restoration: can be considered as inverting the dosages caused by a processor software. We rely on mathematical or probabilistic models for the degradation of an image; and

4. image segmentation: dividing the image into distinct elements or partitioning the image into objects. In this chapter, we discuss the medical and biological image and related topics such as classification of security of these data, the problem of security.

Keywords: digital image, medical image, biological image, encryption, decryption, evaluation parameters

1. Introduction

With the rapid development of multimedia technologies and communication networks and the evolution of equipment that is capable of acquiring, archiving and to transmit images and

videos at reasonable costs, which favours their use in several areas such as computer vision, medical imaging, multimedia systems, satellite imagery, telemedicine, and so on. These data are exchanged via channels that are not always secure, most of them are transmitted over open networks, much of this information is confidential or private. Indeed, this data can be easily intercepted or modified by attackers or by unauthorised users. The security of this information during transfer or storage has become more important and has attracted a lot of attention.

The use of medical imaging and biological image by professionals has remarkably evolved in recent years due to the development of digital technologies. It allows an increasingly in-depth investigation of organs through more efficient radiology systems. The statistical approach induced by the use of computer tools induces treatments on images in very high definition, so a modality like a scanner produces images of the size of the order of 10 MB and a complete examination reaches 500 MB. This critical volume not only posed the problem of the storage, circulation and exchange of this digital information between professionals, but also raised security problems.

2. Digital image

Long before the invention of the computer, the man had chosen a simple way of communication that does not require any specialised knowledge except that of to draw, this method is to draw and design images. First of all, let us agree on the term 'image', the definition of model in the dictionary: [A representation of the external form of a person or thing in art]. For a computer, the display support of a digital image is the screen.

The development of communication media and storage media has dramatically transformed the means of communication. New technologies are mostly based on the exchange and storage of multimedia data and especially digital images. As a result, the digital image becomes plenty. Moreover, it is indispensable in several fields, notably communication [1]. In this section, we study the major categories of images and medical image and biological image. Also, we present the most well-known evaluation parameters of encrypted images.

A colour digital image is a computer file, which can be opened with an image viewing program. Once the image is open in real size, it is in the form of a rectangle consisting of a set of coloured points. A digital image is saved as a file. It is characterised by three elements:

1. Its type and format.
2. Its resolution in pixels.
3. Its colour depth.

2.1. The matrix image

This type of images are prevalent and the most widespread, a digital image matrix, also called the BITMAP image, can be considered as a matrix or an ordered set of two- or three-dimensional digital data.

The row and column indices identify the points in the image. The elements of the matrix are the elementary units of the image, they are called pixels or picture elements; the pixel is an abbreviation for PICture ELement [1, 2]. The number of rows of this matrix is m, and n represents the number of columns, and the product m × n gives us the size of the image. The resolution of an image is defined by the number of pixels per unit length. Therefore, we can build an image 2D as an array of values in which a position is matched on a plane (x, y) and a colour to visualise the image on an electronic medium.

It is simply a grid of thousands of pixels representing the successive colour points of the image. Each pixel is a very small square having precise coordinates and precise colour, in this way, the image then becomes a grid of pixels. This is the technique used in medical and biological image capture devices and digital cameras or scanners. Bitmap images are fully adapted to the world of photography. On the other hand, the more the quality of the image, the more voluminous is the file. Most popular formats are JPEG, PNG and GIF.

2.2. The vector image

It is a digital image composed of geometric objects and created from mathematical equations (such as a circle, an arc, a curve, a straight line, a polygon) and parameters (like position, dimensions, colour). Each object is defined mathematically by equations and attributes like the position, colour, and so on. For example, the vector image of a circle is defined by type attributes such as centre position, radius and a straight line drawn between the points (x 1, y 1) and (x 2, y 2). We cannot present all the images in a vectorial way, and this is mainly the case of realistic photos that are matrix images. A vector image cannot be displayed directly on a screen. It must be transformed into a matrix type image.

These images are mainly used to make diagrams or plans in industrial software such as Desktop Publishing (PAO), CAD (Computer Aided Drawing), AutoCAD, CATIA, Illustrator and the tools of 3D design (like 3DSMax, Maya). The best-known formats are EPS, EMF and Windows Metafile (WMF).

Unlike matrix images, in the vector image, the positions and colours of the objects are not fixed, and they are calculated dynamically by the viewing software. In other words, to display a line, for example, the software determines the starting point, the point of arrival and the trajectory to follow. Then, it calculates and positions all the pixels necessary to display this line. The same procedure can be used for more complex shapes and colours.

Vector images are rather light, that is, small file size. Also, because they consist only of mathematical entities, they have the famous property of being able to be enlarged without limit, each line and each form being dynamically recalculated (**Figures 1(a), (b)** and **2(a), (b)**). On the other hand, they are rather dedicated to creating relatively simple renderings such as diagrams, etc.

Difficult indeed to create such renderings of landscapes, details, games of shadows with vector image that does not allow realism.

In **Figure 1**, we see that when we make a zoom on matrix image, the quality and the clarity of the zoomed image will be decreased. On the other hand, in **Figure 2**, when we zoom a vector image, the zoomed image does not lose the quality.

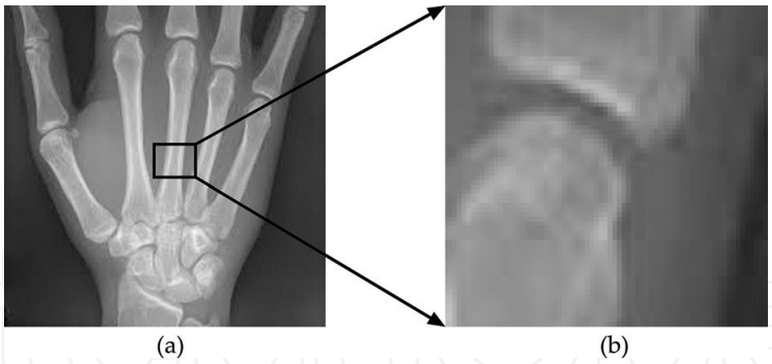

Figure 1. Zoom on matrix image: decrease of the quality of the image.

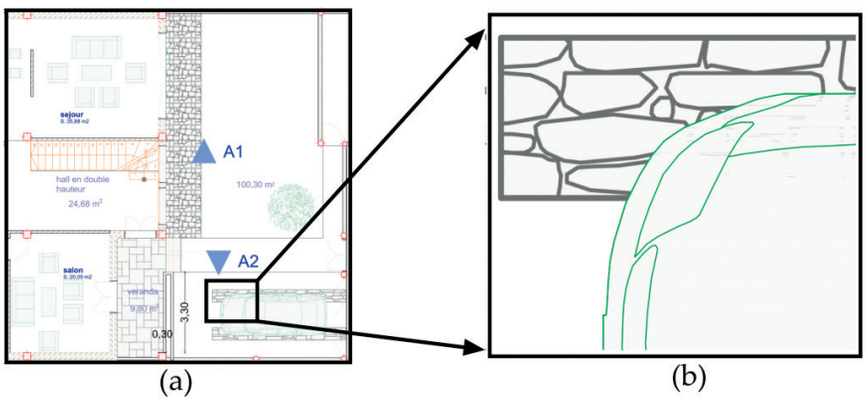

Figure 2. Zoom on vector image: does not lose the quality of the image.

3. Medical and biological image

Medical and biological imaging is a set of techniques consisting of imaging the different regions of the body. The use of the medical and biological images allows a deeper and deeper investigation of organs through radiology, and it is also used in biomedical research to understand better how the body works.

The beginning medical imaging is the result of the work of Wilhelm Röntgen on the X-rays in 1895, and he made the first anatomical X-ray images of his wife Anna Berthe Roentgen. He received the Nobel Prize in Physics in 1901. There exist several types of medical and biological imaging that are more or less adapted according to the area of study. We distinguish in particular [3, 4]:

1. **Images of gamma rays:** the biological body is injected with radioactive isotopes that emit gamma rays, and the emissions are collected with detectors to produce an image.
2. **Radiology, which uses X-rays:** X-rays are one of the oldest sources of electromagnetic radiation used in medical and biological imaging. It is used for diagnostics and also in industry and astronomy.

3. **Magnetic resonance imaging (MRI):** it is a powerful medical diagnostic technique that provides three-dimensional images in an anatomically accurate cut. These examinations use ultrasound, sound waves at very high frequencies (above 20,000 Hz). MRI is based on the physical phenomenon of nuclear magnetic resonance. It is simply a question of observing the nuclear magnetic resonance of the protons of the water contained in the organism.

Medical and biological images are real images, they cannot be calculated; therefore, they are matrix images. The evolution of multimedia and communication technologies has consequences in the field of health through the provision of new means of sharing and remote access like picture archiving communication systems (PACS) and the adoption of new standards. The need for a measure appeared after the development of the media digital and image networks. The medical community has actively set standards for digitally exchanging patient records and in particular, medical images, among the objectives of these criteria, to make the software solutions more efficient. A standard of medical information exchange is a convention between professionals to access and exchange and secure the data. Among the criteria existing on the market, it is possible to quote [4, 5]:

1. Digital Imaging and Communication in Medicine (DICOM):

   Digital Imaging and Communication in Medicine (DICOM) is the global standard for the management of medical images and their environment, and it was created in 1985 by the American College of Radiology (ACR) and the National Electric Manufacturers Association (NEMA) to standardise the data transmitted between different radiology devices [6]. This standard not only defines a file format but also a data transmission protocol. The DICOM standard is now used by most manufacturers of medical imaging equipment.

2. Integrating the Healthcare Enterprise:

   Integrating the Healthcare Enterprise (IHE) is an initiative of health professionals to ensure better interoperability between systems [7]. It proposes the use of standards for the exchange of clinical and administrative information such as DICOM for the image and health level 7 (HL7) for messages between medical software.

3. Hospital Information Systems:

   Hospital Information Systems (SIH) is an information system applied to health facilities such as hospitals, clinics, radiology centres, analysis centres and medical offices? It covers all the systems of functioning in a health facility such as administrative system, accounting system, logistics and stock system, medical informatics, and so on.

4. Radiological Information Systems:

   Information system is usually computer-assisted, designed to store, manipulate and search for information. It manages the planning and management of certain administrative and clinical activities such as patient identification and follow-up, appointment management, the realisation of the exams, dictation of the report, invoicing, and so on.

5. Health Level 7:

   Health Level 7 (HL7) is a standard that defines a format for exchanged clinical electronic data [8]. This information can be financials or administrative.

3.1. Colour coding

For a digital image, we can distinguish three main types of colours [1] (**Figure 3**):

(a) **(b)** **(c)**

Figure 3. (a) Binary image, (b) greyscale image and (c) colour image.

3.1.1. Binary images

Binary images are pixel matrices where the content of each element can only take values 0 for black or 1 for the white colour (**Figure 3(a)**). Therefore, the number of colours is only of two, and the rendering of the image is sometimes sufficient in some cases.

The first applications adapted well to this type of images. In the beginnings of digital image processing, we have the problem of calculation time and memory space. Therefore, it did not allow processing of complex images. Binary images are a simple context allowing formalisation of mathematical problems by tools such as topology. Also, in the field of industrial vision such as fault detection, quality control, measurement, and so on, we often consider the binary image as a mandatory step, generally following the phase of segmentation, hence the importance of this type of images.

3.1.2. Grayscale images

Greyscale images are coded on 8 bits (corresponding to 1 byte), and in this case, we get $2^{24} = 256$ intensities between 0 and 255 which represents, respectively, black and white (**Figure 3(b)**). It is an image that offers several levels of intensity ranging from black to white. Greyscale coding offers more shades than simple black and white. A total of 255 different grey levels are sufficient for the presentation of most medical and biological objects, the advantage of greyscale images is it occupies less space, and the treatment is fluid.

3.1.3. Colour images

In this coding, the image is broken down in general into three planes: red, green and blue (**Figure 3(c)**). The colour of a pixel is obtained, as the painter would mix the basic colours. Each pixel is represented by a vector consisting of red, green and blue components.

We describe one of the most commonly used principles. RGB coding: The principle consists of mixing the three colours: red, green and blue (denoted RGB) (see **Table 1**). With these three colours, we obtain a whole palette of shades ranging from black to white. Each colour is associated with 1 byte (256 levels of brightness) of each of the fundamental colours.

Red	Green	Blue	Colour
0	0	0	Black
255	0	0	Red
0	255	0	Green
0	0	255	Blue
128	128	128	Grey
255	255	255	White

Table 1. Principle of RGB colour coding.

A 'colour' pixel is then coded with 3 (or 24-bit) bytes, and then, it is possible to obtain colour possibilities, that is, 16 million different colours (16,777,216 = 2^{24}).

There are other types of encoding colours, and the best known are TSL, CMY, CIE, YUV, and YIQ.

4. Evaluation methods

Any image processing changes the pixels relative to the original image. A robust ciphering algorithm must make these changes irregularly and at the same time, maximise the difference between the pixel values of the original image and the ciphered image. The encrypted image must be independent of the original image, and the final image must not reveal the characteristics of the plaintext image.

One of the oldest and best-known measures is visual inspection; with the advancement of cryptanalysis techniques, the visual inspection is no longer sufficient to examine the power of a ciphering algorithm. Therefore, the use of quantitative factors is necessary to judge a cryptosystem [9] better.

Factors that measure the quality of the recording techniques can be classified into two families [4, 10]:

1. **Correlation:** This family measures the ability of the algorithm to have a weak relationship between the original image and the encrypted image. In this way, five measures are studied: the histogram, the correlation coefficient, entropy, irregular gap and noise resistance.
2. **Diffusion:** This second family evaluates the characteristics of diffusion of the algorithm. In this family, two measures number of pixels change rate (NPCR) and unified average change intensity (UACI) are studied

4.1. Histogram

The histogram of an image is a discrete function that represents the distribution of the number of pixels in an image; according to their intensity of each value, we associate the number of pixels in the image with this level. It indicates for each value between the black (0) and the white (255), how many pixels of this value in the image; in the abscissa (x-axis): the grey level (from 0 to 255); on the ordinate (y-axis): the number of pixels (see **Figure 4**). In a histogram, each vertical bar represents the number of times of level of corresponding grey [11]. For a digitally reliable algorithm, the histogram of the ciphered image must have both properties:

1. The histogram of the ciphered image must be entirely different from the histogram of the original image.
2. To prevent information leakage to an adversary, the histogram of the ciphered image must have a uniform distribution. **Figure 5** shows the histogram of an encrypted image, and we notice that the number of each intentionality (grey level) is close. We find not a higher intensity in a remarkable way or lower remarkably, so the attacker will not be able to have information on the number of the intentionality of the original image.

4.2. The correlation coefficient

The correlation coefficient (CC) determines the relationship and degree of similarity between two variables. In a cryptosystem of images, the correlation is used to measure the difference between two images [4, 12], the relationship between the pixels at the same location in the

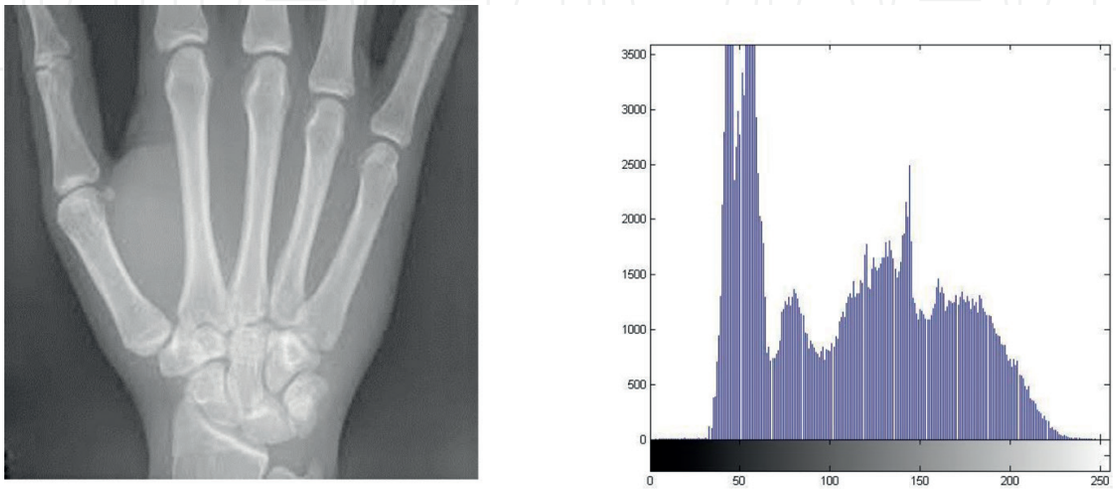

Figure 4. Histogram of greyscale image.

http://dx.doi.org/10.5772/intechopen.75491

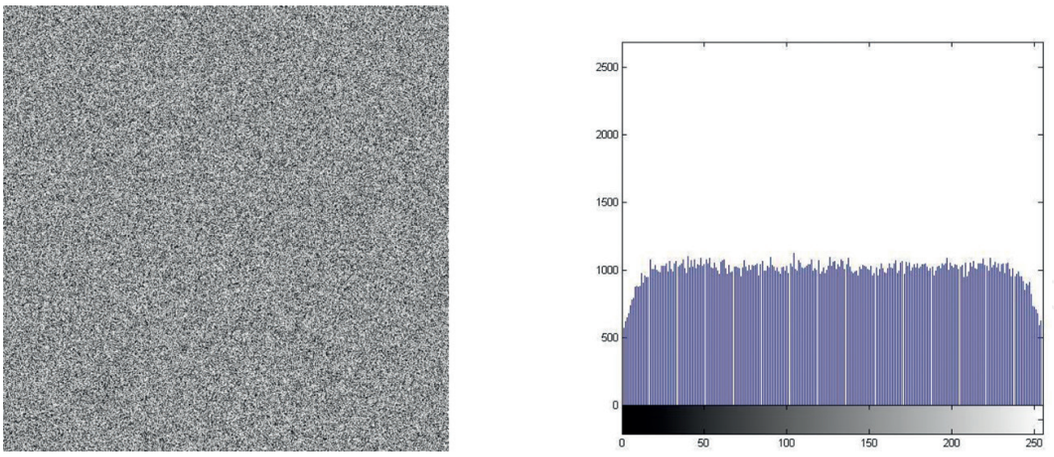

Figure 5. Histogram of ciphered image.

manifest image and the ciphered image. The correlation is a useful measure for judging the quality of the cryptosystem [12, 13].

For a robust cryptosystem, the correlation coefficient (CC) must be very close to zero. Thus, the success of the encryption process signifies small values of CC, and the encrypted image is random and highly uncorrelated [12]. It guarantees that the algorithm is resistant to pixel correlation attack. If the correlation coefficient is close to one, it means that the original image and the ciphered image are very dependent, and the encryption process has failed to hide the details of the original image so that the precise image can be reproduced easily from the encrypted image [12].

The correlation coefficient can be obtained from the formula [11, 12]:

$$CC = \frac{\operatorname{cov}(x, y)}{\sigma_x \sigma_y} = \frac{\sum_{n=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{n=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{n=1}^{N}(y_i - E(y))^2}} \tag{1}$$

where x and y are pixel values of the same index of the original image and the ciphered image, respectively.

4.3. Entropy analysis

The entropy of information is another important factor in evaluating the resistance of a cryptographic system. The entropy of the information H (s) of a source s can be calculated by the formula [14]:

$$H(s) = \sum_{n=0}^{2N-1} P(s_i) \log_2 \frac{1}{P(s_i)} bits, \tag{2}$$

where the probability of the symbol s_i, in the case of greyscale image is:

$$P(s_i) = \frac{the\ number\ of\ s_i\ in\ the\ ciphered\ image}{2^N} \tag{3}$$

By entropy, we can assess the degree of uncertainty and the randomness of the system [15]. If all the symbols 's_i' have the same probability.

4.4. The irregular deviation

The previous parameters are useful for judging the quality of an algorithm, but they are not good enough because they do not keep any information about pixel positions. A suitable encryption algorithm should change the positions of the pixels randomly and uniformly. This avoids the situation in which some pixels will be subject to a significant change then the other pixels will be subject to a small change [4].

The irregular gap is based on the calculation of the divergence caused by the encryption process [16]. The calculation of the irregular deviation (ID) is summarised in the following steps [4, 12]:

1. Find the matrix D which represents the absolute difference between the value of the pixels before and after the encryption: $D = | I - J |$.
2. Construct the histogram 'H' of the matrix D.
3. Find the average value M_H of the histogram H:

$$M_H = \frac{1}{256} \sum_{i=0}^{256} h_i \tag{4}$$

4. Estimate the absolute difference H_D between the histogram and the average value M_H

$$H_D(i) = | h_i - M_H | \tag{5}$$

5. The irregular deviation (ID) is calculated as follows:

$$ID = \sum_{i=0}^{256} H_D(i) \tag{6}$$

The intermittent deviation (ID) indicates the divergence that has the pixel of the original image [12]. If the irregular deviation is close to a distribution uniform, so this is a good parameter of resistance against statistic attacks [4].

4.5. Noise resistance

Noise is present in most of the images; a good cryptosystem must be robust against noise. If the decrypted image is very similar to the original image, then the encryption system is resistant to noise. To measure the noise, we compare the peak signal-to-noise ratio (PSNR) of the original image and the encrypted image, the PSNR is given by the formula [12]:

$$PSNR = 10 \times \log_{10} \frac{255 \times 255 \times M \times N}{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(P_{ij} - Q_{ij}\right)^2} (db) \tag{7}$$

where P_{ij} and Q_{ij} are the pixels of line i and column j of the original image and the ciphered image, respectively, M is the number of rows and N is the number of columns of the image.

4.6. NPCR and UACI

In cryptography, diffusion is a desirable property that is introduced by Shannon in his paper published in 1949 [17]. A good cryptosystem must ensure proper dissemination. Diffusion means that if only one bit of the original image is modified, it should entirely unpredictably change the encrypted image. This phenomenon is also called the avalanche effect.

A suitable algorithm must be susceptible to small changes [18]. The hacker can make a little difference in the original image, and then observe the change result. In this way, if the diffusion parameters are low, it can find a significant relationship between the original image and the encrypted image. If the algorithm has an excellent diffusion, the relationship between the encrypted image and the original image is too complicated, and the attacker cannot easily predict the changes. Therefore, this attack would become inefficient.

To measure the difference in a cryptosystem, we modify a bit in the clear image and then calculate the resulting deviation of the encryption process. To test the influence of this change, two measures can be used: NPCR and UACI [11, 12, 19].

We take two encrypted images, C_1 and C_2, the corresponding original images have a single pixel difference. We also define a matrix D that has the same size as C_1 and C_2:

$$D(i,j) = \begin{cases} 0, & if\ C_1(i,j) = C_2(i,j) \\ 1, & if\ C_1(i,j) \neq C_2(i,j) \end{cases} \tag{8}$$

The first measure is the number of pixels change rate (NPCR) is defined by the formula:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{9}$$

where M and N are the width and height of C_1 and C_2, respectively. The NPCR measures the percentage of different pixels in the two images. The NPCR can also be defined by the variance rate of the pixels in the encrypted image caused by the change of a single pixel in the original image.

The second measure is the unified average change intensity (UACI) is defined by:

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \tag{10}$$

5. Cryptology

Significant progress in technology and the enormous amounts of data generated digital births have given rise to new problems. Of these issues, there is data protection or cryptography. Cryptography uses the mathematics to transform a data in the clear into an incomprehensible data, and the opposite direction of this operation is cryptanalysis. Therefore, cryptology has two main branches: cryptography and cryptanalysis. Encryption is the secret writing of information, and cryptanalysis is the analysis of cryptography or the study of the level of security of the systems.

The purpose of cryptography is to provide some security services such as confidentiality, integrity and authenticity [20, 21]. The word cryptography comes from Greek 'Krypto' means I hide and 'graph' means document [22].

Cryptography is not used solely to protect the diplomatic and military communication. Nowadays, image encryption has applications in various fields such as medical and biological image, internet communication, closed-circuit television (CCTV), satellite image, and so on.

In this section, we study the two main branches of cryptology:

5.1. The objectives of cryptography

Cryptography is the study of the techniques used to accomplish the four following purposes [20, 21]: confidentiality, integrity, authentication and nonrepudiation.

Confidentiality: confidentiality is to prohibit access to unauthorised entities.

Integrity: data integrity ensures that information has not been changed between the sender and the receiver.

Authentication: ensure the identity of a person wishing to access this data.

Nonrepudiation (traceability): is to trace any action on the documents. It is a way of preventing an entity from denying participation in an electronic exchange.

5.2. Classification of algorithms

Encryption algorithms can be classified in different ways; according to the structure of the algorithms, depending on the keys or the percentage of the encrypted data [4] (**Figure 6**).

Classification according to the keys: in general, there are three types of encryption systems such as symmetric, asymmetric and hashing:

1. **Symmetric encryption:** also called 'Secret Key Encryption'. The same key is used to write and decrypt, the sender and the recipient must share the same key to perform encryption and decryption. Bob and Alice have to share the secret key via a secure channel to be able to hide the encrypted messages (see **Figure 7**).
2. **Asymmetric encryption:** (public key encryption) is a system where the sender and recipient have a key pair, a public for encryption and a private one for the decryption. Alice uses Bob's public key to encrypt a message for Bob. Bob uses his private key that is not shared to decipher Alice's message (see **Figure 8**).
3. **Hash functions:** a mathematical function that associates a data with a fixed size output is called a hash function. The hash must be unique and short, the return of the hash to the original data must be impossible (see **Figure 9**).

Classification according to the encryption structure: in modern symmetric cryptography, the encryption algorithms can be classified according to the structure into two broad categories: encryption by blocks and stream ciphering.

http://dx.doi.org/10.5772/intechopen.75491

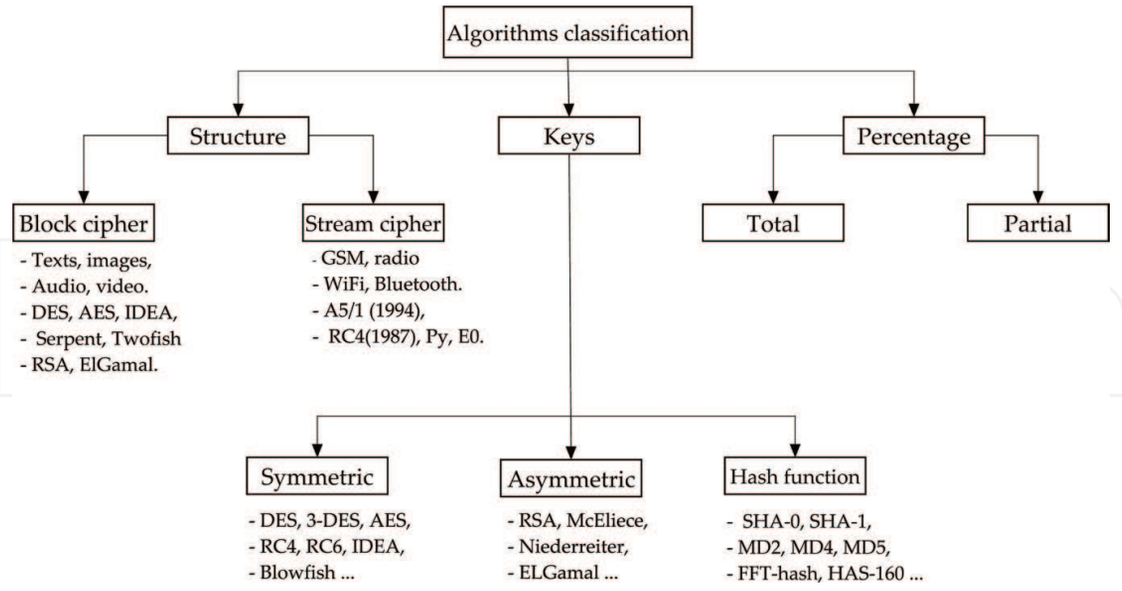

Figure 6. Classification of algorithms.

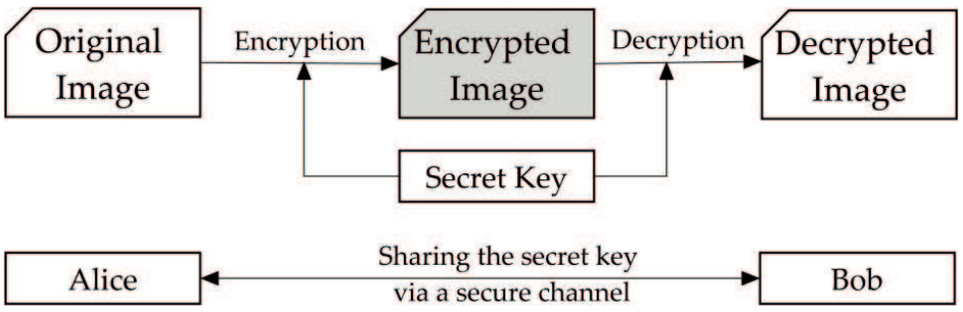

Figure 7. Symmetric encryption.

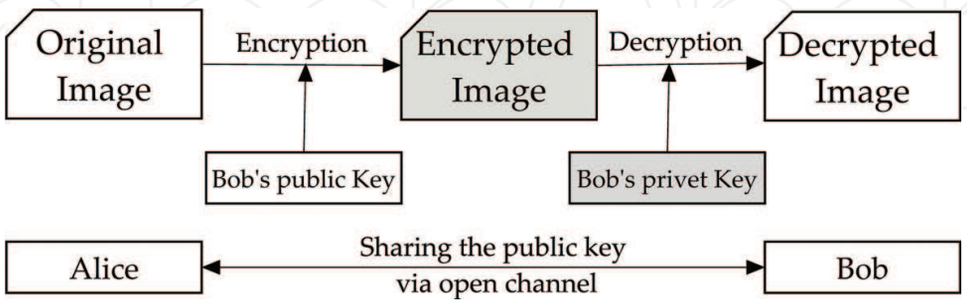

Figure 8. Asymmetric encryption.

1. **Block cypher** has a simple principle, cutting data into blocks fixed size.
2. **Stream cypher**: is to encrypt the bits individually, it is designed to be faster than block cypher and economical regarding resources.

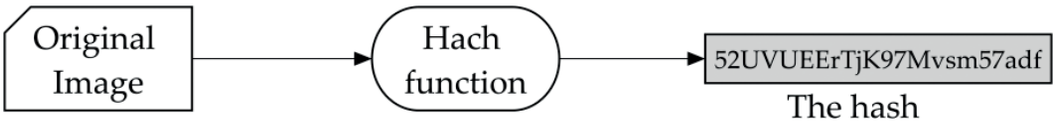

Figure 9. Hash function.

Classification by percentage of encrypted data: depending on the interest of the encrypted data, the encryption can be divided into two groups: total encryption and partial encryption.

1. **Total encryption:** Consists of encrypting all bits of the data, consumes more resources, it is expensive regarding the time of calculation.
2. **Partial encryption:** Or selective is a recent approach that aims to reduce the computing time. It consists of encrypting only a subset of the data. For medical and biological images, to have a reasonable level of confidentiality, at least 12.5% of the data must be encrypted [23, 24].

5.3. Electronic signature

An exciting application of public key cryptography is the digital signature, which is the reverse use of public key encryption. The digital signature is used in the opposite direction of an asymmetric encryption algorithm (**Figure 10**).

5.4. Cryptanalysis

If decryption is to find the precise text knowing the key and the algorithm, cryptanalysis is to try to find the exact version without knowing the key. Cryptanalysis or what Oscar does is the science or art of deciphering encrypted data when the key is unknown. It was developed parallel to cryptography. Among the objectives of cryptanalysis is to measure the weaknesses and robustness of the capacity of a cryptosystem to attack [21, 25].

The primary types of cryptanalysis: According to the information known by the cryptanalysts, we can distinguish the various basic types of cryptanalysis (non-exhaustive list) [21]:

1. **Ciphertext-only attack:** the attacker only has access to encrypted texts of several messages and tries to analyse them to deduce the key or discover the plaintext.

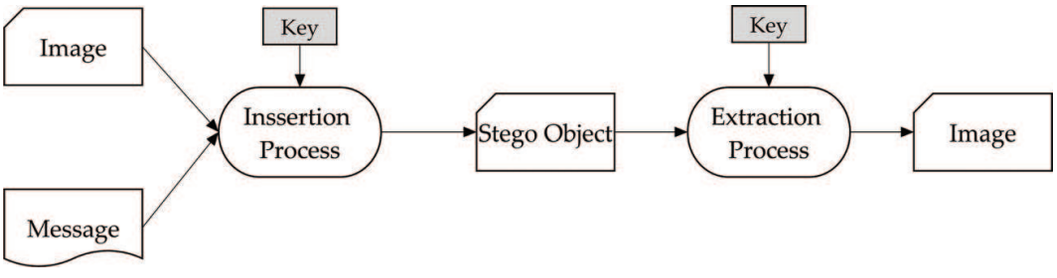

Figure 10. Electronic signature.

2. **Known-plaintext attack:** The adversary knows both parts of the ciphertext and the corresponding plaintext.

3. **Chosen-plaintext attack:** the cryptanalyst has access to the algorithm or the encryption machine, and he/she chooses plain texts and produces the encrypted version of this text. The opponent can use the pairs of clear and encrypted messages to obtain the secret key.

4. **Chosen-ciphertext attack:** The enemy has access to the device of decryption; it has the possibility of choosing the texts to be deciphered without knowing the key.

5. **Brute-force attack:** the attacker tries all combinations of possible keys until the acquisition of the plaintext.

6. Conclusion

In this chapter, we have presented generalities on digital image and medical and biological image, cryptography, primary themes used in encryption, the objectives of cryptography and the classification of algorithms, this ranking is non-exhaustive, there are other types of algorithms like chaotic algorithms [26], as its name suggests, chaotic cryptography relies on the use of chaos. The theory of elliptic curves and the approach of correcting codes are also used to develop new public vital algorithms [27].

We have also mentioned in this chapter the second branch of the cryptology: cryptanalysis, its principles and the different types of attacks. The creation of modern encryption techniques has brought light to new methods of cryptanalysis. We can group these new methods into two large families: differential cryptanalysis [4] and linear cryptanalysis [21].

Graph colouring problem steganography and watermarking can also be a solution to increase safety [12, 24]. Steganography is a technique used to hide secret data in media imperceptibly (**Figure 11**). Many effective steganographic methods can be found in the literature [28]. The primary purpose of watermarking is the protection of copyright by adding visible or nonvisible copyright information. We can find several stenographic techniques [28, 29] and watermarking techniques [30] in the literature.

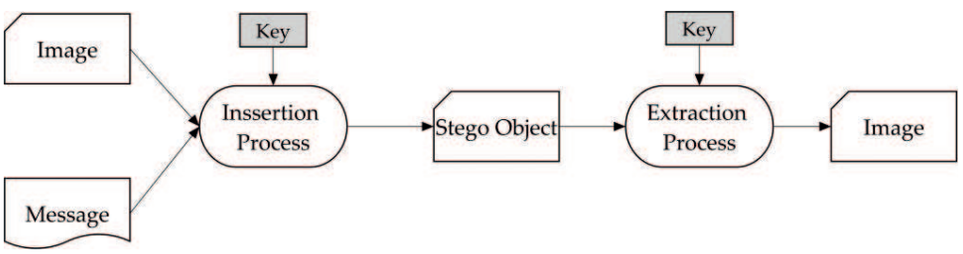

Figure 11. Steganographic scheme

Author details

Abdelkader Moumen

Address all correspondence to: abdelkader.moumen@gmail.com

Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

References

[1] Gonzalez RC, Woods RE. Digital Image Processing. 2nd ed. Addison-Wesley; 1993

[2] Salles D. Éducation à L'image et aux Médias: La Liberté de la Presse. Centre de Ressources en éducation aux médias CREM; 2005

[3] Gkoulalas-Divanis A, Loukides G. Medical Data Privacy Handbook. Switzerland: Springer International Publishing; 2015. 832 p. ISBN: 978-3-319-23633-9

[4] Moumen A. Imagerie médicale et stockage numériques sécurisées [thesis]. Annaba, Algeria: Badji Mokhtar University; 2017

[5] Calcote S. Developing a secure healthcare information network on the Internet. Healthcare Financial Management. 1997;**51**(1):68

[6] Digital Imaging and Communications in Medicine. http://medical.nema.org/

[7] Integrating the Healthcare Enterprise. http://www.ihe.net/

[8] Health Level Seven. https://www.hl7.org/implement/standards/

[9] Dey S. SD-AEI: An advanced encryption technique for images. In: Second International Conference on Digital Information Processing and Communications (ICDIPC2012). Lithuania: IEEE; 2012. pp. 68-73

[10] Pandey V, Singh A, Shrivastava M. Medical image protection by using cryptography data-hiding and steganography. International Journal of Emerging Technology and Advanced Engineering. 2012;**2**(1):106-109

[11] Li SJ, Chen GR, Zheng X. Chaos-based encryption for digital images and videos. In: Multimedia Security Handbook. 2004

[12] Moumen A, Sissaoui H. Images encryption method using steganographic LSB method, AES and RSA algorithm. Nonlinear Engineering - Modeling and Application. 2016;**6**(1): 53-59. DOI: 10.1515/nleng-2016-0010

[13] Elashry I, Allah O, Abbas A, El-Rabaie S, El-Samie F. Homomorphic image encryption. Journal of Electronic Imaging. 2009;**18**:033002

[14] Han Z, Feng W, Hui L, Da Hai L, Chou L. A new image encryption algorithm based on chaos system. In: 2003 IEEE International Conference on Robotics, Intelligent Systems and Signal Processing. Vol. 2. IEEE; 2003. pp. 778-782

[15] Shu-Jiang X, Ying-Long W, Ji-Zhi W, Min T. A novel image encryption scheme based on chaotic maps. In: 9th International Conference on Signal Processing, 2008 (ICSP 2008); IEEE; 2008. pp. 1014-1018

[16] Ziedan IE, Fouad MM, Salem DH. Application of data encryption standard to bitmap and JPEG images. In: Proceedings of 12th National Radio Science Conference (NRSC2003); 2003. pp. C16/1-C16/8

[17] Shannon C. Communication theory of secrecy systems. Bell System Technical Journal. 1949;**28**(4):656-715

[18] Lian S. Multimedia Content Encryption: Techniques and Applications. London: Taylor & Francis Group, LLC; 2009

[19] Hennelly BM, Sheridan JT. Image encryption based on the fractional Fourier transform. Proceedings of SPIE. 2003;**5202**:76-87

[20] Schneier B. Applied Cryptography. Second ed. New York: John Wiley and Sons; 1996

[21] Stinson D. Cryptography: Theory and Practice. 2nd ed. Boca Raton, USA: Chapman & Hall/CRC; 2002

[22] Singh S. Histoire des Codes Secrets. De l'Égypte des Pharaons à L'ordinateur Quantique. Jean-Claude Lattès; 1999

[23] Spanos GA, Maples TB. Performance study of a selective encryption scheme for the security of networked, real-time video. In: Proceedings of 4th International Conference on Computer Communications and Networks; 1995. pp. 20-23

[24] Moumen A, Bouye M, Sissaoui H. New secure partial encryption method for medical images using graph coloring problem. Nonlinear Dynamics. 2015;**82**(3):1475-1482. DOI: 10.1007/s11071-015-2253-4

[25] Menezes A, van Oorschot P, Vanstone S. Handbook of Applied Cryptography. CRC Press; 1996

[26] Amigó JM. Chaos-based cryptography. In: Intelligent Computing Based on Chaos. Berlin: Springer; 2009. pp. 291-313. ISBN: 978-3-540-95971-7

[27] Miller V. Use of elliptic curves in cryptography in advances in cryptography CRYPTO 85. Lecture Notes in Computer Science. Springer-Verlag. 1989;**218**:417-426. 2, 6

[28] Bender DW, Gruhl NM, Lu A. Techniques for data hiding. IBM Systems Journal. 1996; **35**:313-316

[29] Provos N. Universal Steganography. Août 1998. http://www.outguess.org/

[30] Cayre F, Fontaine C, Furon T. Watermarking security: Theory and practice. IEEE Transactions on Signal Processing. 2005;**53**(10):3976-3987

IntechOpen