CHAPTER II

LITERATURE SURVEY ON IMAGE ENCRYPTION

2.1. Overview

During the last two decades, computer networks created a revolution in the use of information. Authorized people can send and receive information from a distance using computer networks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity, when it is needed (availability). [14] Transmitted information over computer networks nowadays is not only textual data, but also multimedia data such as audio, image, video and other multimedia types. The security of multimedia has matured in the last few years to provide a class of tool-sets and design insights for the protection and enhancement of digital media under a number of diverse attack scenarios. In such a setting, one natural question that arises is the security and confidentiality of a digital packet of multimedia information. [15]

This chapter provides a detailed description of the cryptographic systems used in this research. Section 2.2 presents the general aspects of the digital images and their format. Section 2.3 defines the fundamental concepts of cryptography systems and image encryption. Section 2.4 explores the classification of encrypting algorithms. Section 2.5 presents the basic concepts of image encryption and decryption. Section 2.6 explains the image security measurements, the correlation among image elements, image entropy, image similarity in a certain degree of details and image histogram. These security measurements will be used in this research to compute and evaluate the encrypted images produced by the combination technique. Section 2.7 demonstrates an overview of soft computing, its tools and its applications. This chapter also introduce brief information on image encryption using soft computing. Section 2.8 displays a literature review on image encryption using soft computing algorithms (fuzzy logic and genetic algorithm). Finally, section 2.9 summarizes the main points presented and discussed in this chapter.
2.2. Digital Images

Digital image can be defined as “an image consisting of data (specifically a set of elements) based on an $n$-dimensional regular grid that has the potential for display. These elements are referred to as pixels. The pixels in different images may represent a variety of types of information, such as temperature, pressure, velocity, terrain height, or tissue density”. [16] The regular grid is frequently over a two-dimensional space but can be three-dimensional, and even four-dimensional if sampling over time is also included. In real world applications, digital images are visually displayed by pixel values which represent various colours. A digital image is defined as an array of individual pixels and each pixel has its own value. The array, and thus the set of pixels, is called a bitmap. Figure 2.1 shows an example of images represented by different number of colours depending on the number of bits used for each pixel. The three images in the figure 2.1 are of the same size, i.e., 512 rows and 512 columns, denoted by 512x512, for a total of 262144 pixels. The pixel values in a binary image as shown in figure 2.1(a) are any two values in general that are normalized, e.g., 0 and 1 or 0 and 255. The pixel values in a grayscale image as in Figure 2.1(b) are integer values between 0 and 255, which have a total of 256 gray value representations. A multispectral image typically contains information outside the normal human perceptual range. A true colour image as shown in figure 2.1(c) contains three grayscale images as three components: red, green, and blue referring to figure 2.2.

![Image Types](image_url)

**Figure 2.1** Image Types
Digital images are produced through a process of two steps: sampling and quantization. Sampling is the operation of dividing the original image into small parts which are called pixels, whereas quantization is the operation of assigning an integer value (i.e. colour) to each. The number of colours (i.e. colour space) that can be assigned to any picture element or pixel is a function of the number of bits, which is occasionally referred to as the colour depth or bits resolution. This connotation is also known as bits per pixel (bpp) that represents the colour for each value. The colour space is computed using the following equation:

\[ Colour \ Space = 2^b \]  

Where \( b \) is the bit depth.

The colour values used in each bitmap depend on the specific bitmap format. This means that each pixel in a bitmap contains certain information, ordinarily as colour information. The content of information is always the same for all the pixels in a particular bitmap. Thus, each value of colour in a bitmap is a binary number, which is a sequence of binary digits that can be either 0 or 1 and called bits. This binary number in a given format will differ in length depending on the colour depth of the bitmap, where the colour depth of a bitmap determines the range of possible colour values that can be used in each pixel. For instance, each pixel in a 24-bit image can be one of roughly 16.8 million colours. This means that every pixel in a bitmap has three colour values between 0 and 255 and then those colours are formed by mixing together varying quantities of three primary colours: red, green and blue. [17] Table 2.1 demonstrates the image colour space.
Table 2.1 Image colour space versus bit depth (bpp).

<table>
<thead>
<tr>
<th>Image properties</th>
<th>Bits resolution</th>
<th>Colour space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binary image (black and white)</td>
<td>1</td>
<td>2 colours</td>
</tr>
<tr>
<td>Gray scale (monochrome)</td>
<td>8</td>
<td>256 gray levels</td>
</tr>
<tr>
<td>Coloured image</td>
<td>8</td>
<td>256 colours</td>
</tr>
<tr>
<td>Coloured image</td>
<td>16</td>
<td>65536 colours</td>
</tr>
<tr>
<td>True colour (RGB)</td>
<td>24</td>
<td>16,777,216 colours</td>
</tr>
</tbody>
</table>

As seen in Table 2.1 the number of bits increases, the image quality is also increased. However, storage requirements will increase, resulting in a direct relationship between the image storage size and the bits resolution. Image storage size for an uncompressed image is computed using the following equation:

\[ IMGSS = IMGR \times BR \]  

(2.2)

Where, \( IMGSS \) is image storage size, \( IMGR \) is image resolution i.e. (image width \( \times \) image height) and \( BR \) is bits resolution (bits depth). For example, the storage size of a 640 pixels \( \times \) 480 pixels, true coloured image is given as follows:

\[ IMGSS = W \times H \times BR = 640 \times 480 \times 24 \text{ bits} = (7372800/1024/8) = 900 \text{ KB}. \] [18]

2.2.1. Digital Images Formats

In general, there are three types of image files, bitmap, vector and metafiles. When an image is stored as a bitmap file, its information is stored as a collection of pixels, which is manifest as coloured or black-and-white dots. When an image is stored as a vector file, its information is stored as mathematical data. The metafile format can store image information as pixels (bitmap), mathematical data (vector), or both. There is no single format that is appropriate for all types of images. The most common file formats are discussed below:

a) Windows Bitmap (BMP)

The (BMP) is an uncompressed image file format. A pixel value in a gray scale bitmap image is normally represented by 8 bits, i.e., a total of 256 (= 28) combinations of the bits. It may also be represented by other number of bits, such as 16 bits or 32 bits, based on the applications used as well as users’ requirements. In
other words, a gray scale image can be decomposed into eight binary image layers, where each layer is a bit plane and implies a weight. The BMP Bitmaps are defined as a regular rectangular mesh of cells called pixels; each pixel contains a colour value as shown in Figure 2.3. Bitmap are characterized by only two parameters: the number of pixels, and the information content (colour depth) per pixel, and they are the most commonly used type to represent images on the computer.

![Image of pixels](image)

**Figure 2.3 Image’s pixels**

**b) Graphics Interchange Format (GIF)**

The (GIF) Format was originally developed by CompuServe in 1987. It is one of the most popular file formats for web graphics and exchanging graphic files between computers. It is a very common format of images to be used for web images. The GIF format supports 8 bits of colour information that is limited to 8 bits palette and 256 colours. Thus, only 256 different colours are available to represent the picture. It can be viewed by all common browsers. GIF also support animation, transparency and interlacing. GIF images are automatically compressed when they are saved using a lossless compression method known as LZW (Lempel-Ziv-Welch) that does not degrade the image quality.

**c) Portable Network Graphics (PNG)**

The PNG format, a new type of image format, includes a conceptual idea of a fourth component, alpha channel, for having the characteristic of transparency. This allows a PNG image to be incorporated with various backgrounds. The alpha channel is of the
same size as the RGB channels. Each pixel element in the alpha channel can be either binary or one of the 256 combinations, i.e., between 0 and 255.

d) **Joint Photographic Experts Group (JPEG/JPG)**

The (JPEG) format is one of the most popular formats for web graphics. It supports 24 bits of colour information. The JPEG file format stores all of the colour information in an RGB image, and then it compresses the file size to save storage space, or it saves only the colour information that is essential to the image. It is a very common type of image used mostly in web pages, and it is classified as a lossy type of format, using JPG compression, but the compression technique can be selected. We can have a high quality image with a large file size or low quality image with a small file size such as RGB 24 bits. [19] In addition to the mentioned types, there are other types such as:

1) **Encapsulated PostScript (EPS)**

The (EPS) file format is intended to make files usable as a graphics file format. The EPS file format is a metafile format. It can be used for vector images or bitmap images. It can also be used on a variety of platforms, including Macintosh and Windows. If an EPS image is inserted into a document, we can scale it up or down without information loss.

2) **Multispectral Images**

Multispectral images typically contain information outside the normal human perceptual range. This may include infrared, ultraviolet, X-ray, acoustic, or radar data. These are not images in the usual sense because the information represented is not directly visible by the human system. However, the information is often represented in visual form by mapping the different spectral bands to RGB components.
2.3. Basic Concepts of Image Encryption and Decryption

Today, the web is going towards the multimedia data in which image covers the highest percentage of it. But with the ever-increasing growth of multimedia applications, security is an important aspect in communication and storage of images, and encryption is the way to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand and to keep the image confidential between users. In other words, it is important to clarify that without decryption key no one can access the content. Images are widely used in several processes, so the protection of image from unauthorized access is very important. Encryption is the conversion of data into a secret code usable over a general network. Cryptography enables the sender to securely store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. Encryption of sensitive data is necessary. It is used to make the information unintelligible if transmission is intercepted by unauthorized individuals. The intelligible form (original data) of information is called plain text/image and the unintelligible form (protected data) is called cipher text/cipher image. The process of converting the plain text/image into cipher text/image is called encryption, while the inverse process of transforming cipher text/image into the corresponding plain text/image is called decryption. [20]

In general, most encryption algorithms use a secret value called a key. The security of encrypted data entirely depends on two things: the strength of the encryption algorithm and the secrecy of the key. The key is used for encryption and decryption and it must be kept secret, thereby requiring the sender and receiver to agree on the same key before making any data transmissions. The key is independent of the plain text/plain image. Therefore, the same plain text/plain image is encrypted to different cipher text/image with different keys. Thus both processes are impossible to be fulfilled without the use of the correct key. Encryption can be strong or weak. Encryption strength is measured by the time and resources it would require to recover the plain text/plain image. The result of powerful encryption is cipher text/image that is very difficult to decipher without possession of the appropriate decoding tool. The sender and the receiver must keep the key secret because anyone who knows the key can use
it to encrypt the plain text/image. In addition, the strength of the algorithm is important. An unauthorized entity can take encrypted cipher text/image and endeavour to break the encryption by determining the key based on the cipher text/image. While cryptography is the science of securing data, crypt-analysis is the science of analyzing and breaking secure communication, and therefore it is the process of recovering the plain text/image or key, usually by using the cipher text/image and knowledge of the algorithm [21].

Cryptography can also be used to ensure the security of the communication path through the following: (a) data integrity which means ensuring that the data has not been modified by unauthorized entities. Thus, the message received by the receiver is the same as the message sent by the sender. (b) Non-repudiation ensures that the sender of any message cannot deny his/her actions. This can be achieved with digital signatures in conjunction with asymmetric key encryption. (c) Authentication is the process of proving the identity, and (d) privacy/confidentiality is the process to ensure that no one can read the message except the intended recipient [22].

The basic idea of encryption is to modify the message in such a way that only a legal recipient can reconstruct its content. A discrete-valued cryptosystem can be characterized by:

- A set of possible plain texts, P.
- A set of possible cipher texts, C.
- A set of possible cipher keys, K.
- A set of possible encryption and decryption transformations, E and D.

An encryption system is also called a cipher or a cryptosystem. The message for encryption is called plain text/image, and the encrypted message is called cipher text/image. Denote the plain text/image and the cipher text/image by $P$ and $C$, respectively [10].

The encryption procedure of a cipher can be described as:
Encryption and Decryption Image Using Multiobjective Soft Computing Algorithm

\[ C = E_{K_e}(P), \quad (2.3) \]

Where \( K_e \) the encryption is key and \( E \) is the encryption function. Similarly, the decryption procedure is expressed as:

\[ P = D_{K_d}(C), \quad (2.4) \]

Where \( K_d \) the decryption is key and \( D \) is the decryption function. The security of a cipher should only rely on the decryption key \( K_d \), since an adversary can recover the plain text from the observed cipher text once he gets \( K_d \). Figure 2.4 shows a block diagram for encryption/decryption of a cipher.

![Figure 2.4 Encryption/Decryption of a cipher.](image)

The explosive growth in the use of computers for storing information and e-mail for transmitting it and the arrival of e-commerce has made to cryptography becoming an essential feature of modern communications and data storage. Encryption is an area of cryptography involving the transformation of information into some gibberish form, thus ensuring privacy by keeping the information hidden from anyone for whom it is not intended – one may wish to encrypt files on a hard disk to prevent an intruder from reading them, or in a multi-user setting, encryption allows secure communication over an insecure channel. An example of this: A wishes to send a message/image to B so that no one else besides B can read it. A encrypts the message/image (plain text/plain image) with an encryption key; the encrypted message/image (cipher text/cipher image) is sent to B. B decrypts the cipher text/image with the decryption key and reads the message/image.

An attacker, C, may either try to obtain the secret key or to recover the plain text/image without using the secret key. In secure cryptosystem, the plain text/image
cannot be recovered from the cipher text/image except by using the decryption key. Till today, the most successful image encryption scheme is random phase encoding in fractional domain. In this thesis, multi objective soft computing algorithm is used as a modern and high quality method of encryption and decryption images. Therefore, it is impossible to access the image without keys. The significant features of image encryption come from its extra degree of freedom provided by fractional orders.

2.4. Classification of Encryption Algorithms

Encryption algorithms can be classified in different ways; according to structures of the algorithms, keys, or percentage of the data encrypted [23, 24].

2.4.1. Classification According to Encryption Structure

Encryption algorithms can be classified according to encryption structure into block ciphers and stream ciphers. A block cipher is a type of symmetric-key encryption algorithms that transforms a fixed-length block of plain text data into a block of cipher text data of the same length. The fixed length is called the block size. For many block ciphers, the block size is 64 or 128 bits. The larger block size is the more secure. The encryption, decryption algorithms and devices become more complex. Modern block ciphers have the following features: [25]

1. Variable key size.
2. Mixed arithmetic operations, which can provide non-linearity.
3. Data-dependent rotations and key-dependent rotations.
4. Lengthy key schedule algorithm.
5. Variable plain text/cipher text blocks, sizes and variable number of rounds.

Block ciphers can be characterized by:

1. Block size. Larger block sizes mean greater security.
2. Key size. Larger key sizes mean greater security.

3. Number of rounds. Multiple rounds increase security.

4. Encryption modes. They define how messages larger than the block size are encrypted.

Unlike block ciphers that operate on large blocks of data, stream ciphers typically operate on smaller units of plain text, usually bits. So, stream ciphers can be designed to be exceptionally fast, much faster than a typical block cipher. Generally, a stream cipher generates a sequence of bits as a key (called key stream) using a Pseudo Random Number Generator (PRNG) that expands a short secret key (e.g., 128-bits) into a long string (key stream) (e.g., 106 bits), and the encryption is accomplished by combining the key stream with the plain text. Usually, the bitwise XOR operation is chosen to perform ciphering, basically for its simplicity [26-28]. Stream ciphers have the following properties:

1. They don’t have perfect security.

2. Security depends on the properties of the PRNG.

3. The PRNG must be unpredictable; given consecutive sequence of output bits, the next bit must be hard to predict.

4. Typical stream ciphers are very fast.

Today, there is no stream cipher that has emerged as a standard. The most widely used stream cipher is the RC4. The stream ciphers may be employed in many applications such as in Transport Layer Security (TLS), Wired Equivalent Privacy (WEP), etc [29].

2.4.2. Classification According to Keys

According to keys, there are two kinds of ciphers following the relationship of $K_e$ and $K_d$. When $K_e = K_d$, the cipher is called a private-key cipher or a symmetric
cipher. For private-key ciphers, the encryption/decryption key must be transmitted from the sender to the receiver via a separate secret channel. When $K_e \neq K_d$, the cipher is called a public-key cipher or an asymmetric cipher. For public-key ciphers, the encryption key $K_e$ is published and the decryption key $K_d$ is kept private, for which no additional secret channel is needed for key transfer. In conventional encryption as shown in figure 2.5, the sender encrypts the data (plain text) using the encryption key and the receiver decrypts the encrypted data (cipher image) into the original data (plain image) using the decryption key. In symmetric encryption, both encryption and decryption keys are identical. Figure 2.6 shows the public key encryption (asymmetric encryption), in which the encryption and decryption keys are different. Instead of one key, there are two different keys; a public ($K_e$) and a private ($K_d$). Public key cryptography solves the problem of conventional cryptosystems by distributing the key [30-33].

In general, there are two types of cryptosystems:

(1) Symmetric (private) key cryptosystems.

(2) Asymmetric (public) key cryptosystems.

Most people have chosen to call the first group simply symmetric key cryptosystems, and the popular name for the second group is just public key cryptosystems.

![Figure 2.5 Model of symmetric encryption.](image-url)
2.4.3. Classification According to Percentage of Encryption Data

With respect to the amount of encrypted data, the encryption can be divided into full encryption and partial encryption (also called selective encryption), according to the percentage of the data encrypted.
2.5. Basic Encryption Techniques

Basically, cryptographers depend on the type of transformation and the keys to divide the encryption algorithms. Some algorithms require prior agreement on secret key irrespective of the normal communication protocol. Encryption techniques are very useful tools to protect secret information. Encryption will be defined as the conversion of plain message into a form called a cipher text that cannot be read by any people without decrypting the encrypted text. Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be read. The image encryption algorithms can be classified into three major groups: (i) Position permutation based algorithm, (ii) Value transformation based algorithm and (iii) Visual transformation based algorithm [34-37]. Modern cryptography concerns itself with the following four objectives:

- Confidentiality: The information should be kept secret.
- Integrity: The information should not get altered in storage or transit.
- Non-repudiation: The intentions of sender or receiver should not be changed at later stage.
- Authentication: The sender and receiver should confirm each other.
- Key Management: Distribution of secret keys for encryption and decryption.

Image encryption has some applications in the internet communication, multimedia systems, medical imaging, telemedicine, military communication and so on. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost much greater than that of text. Therefore, the old system takes more time for encrypting the image data directly. The other reason is that the decrypted text must be equal to the original text. The image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. Image encryption, video encryption and the image data have special properties such as bulk capability, high redundancy and high correlation among the pixels.
2.6. Measurements of Image Security

In this section, we will discuss, in details, two families of encryption metrics. The first family evaluates the ability of the encryption algorithm to substitute the original image with uncorrelated encrypted image. In this family, five metrics—histogram deviations DH, the correlation coefficient \( r_{xy} \), the irregular deviation DI, the histogram uniformity, and a proposed encryption quality metric—are studied. The second family evaluates the diffusion characteristics of the encryption algorithm. In this family, three metrics—the Avalanche effect, NPCR and UACI—are studied.

2.6.1. Image Correlation Coefficient

A useful measure to assess the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the plain and the cipher images. This metric can be calculated as follows:

\[
C_r = \frac{N \sum_{j=1}^{N} (X_j \cdot Y_j) - \sum_{j=1}^{N} X_j \sum_{j=1}^{N} X Y_j}{\sqrt{(N \sum_{j=1}^{N} X_j^2 - (\sum_{j=1}^{N} X_j)^2) \cdot (N \sum_{j=1}^{N} Y_j^2 - (\sum_{j=1}^{N} Y_j)^2)}}
\]  

(2.5)

Where \( X \) and \( Y \) are the values of two adjacent pixels in the image and \( N \) is the total number of adjacent pixels selected from the image.

Where \( L \) is the number of pixels involved in the calculations. The closer the value of \( r_{xy} \) to zero is, the better the quality of the encryption algorithm will be. [38]

2.6.2. Image Histogram

A histogram uses a bar graph to profile the occurrence of each gray level of the image. The horizontal axis represents the gray-level value. It begins at zero and goes to the number of gray levels. Each vertical bar represents the number of times of corresponding gray level occurred in the image [25].
For image encryption algorithms, the histogram of the encrypted image should have two properties:

1. It must be totally different from the histogram of the original image.

2. It must have a uniform distribution, which means that the probability of existence of any gray scale value is the same, and it is totally random.

2.6.3. The Histogram Deviation

The histogram deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images [38]. The steps of calculating this metric are:

1. Estimate the histogram of both the original and the encrypted images.

2. Estimate the absolute difference between both histograms.

3. Estimate the area under the absolute difference curve, divided by the total area of the image, as follows:

\[
D_H = \frac{\frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i}{MN}
\]  

(2.6)

Where \(d_i\) is the amplitude of the absolute difference curve at the gray level i. \(M\) and \(N\) are the dimensions of the image to be encrypted. The higher the value of \(D_H\) is, the better the quality of the encrypted image will be. [25] Although this measure of quality will give good results about how the encrypted image is deviated from the original image, it can not be used alone to measure the quality of encryption as it has some limitations as will be explained later. Although this measure of quality will give good results about how the encrypted image is deviated from the original image, it can’t be used alone to measure the quality of encryption.
2.6.4. Image Similarity

It is a common task in image analysis to compare how similar two images might be. This comparison may be limited to a particular region of each image. Image Similarity Metrics are methods that produce a quantitative evaluation of the similarity between two images or two image regions. These techniques are used as a base for registration methods because they provide the information that indicates when the registration process is going in the right direction. A large number of Image Similarity Metrics have been proposed in the medical image and computer vision community. There is no a right image similarity metric but a set of metrics that are appropriated for particular applications. Metrics fit very well the notions of tools in a toolkit. You need a set of them because none is able to perform the same job as the other.

2.6.5. Image Entropy

Image entropy is a quantity which is used to describe the ‘businesses of an image, i.e. the amount of information which must be coded for by a compression algorithm. Low entropy images, such as those containing a lot of black sky, have very little contrast and large runs of pixels with the same or similar DN values. An image that is perfectly flat will have an entropy zero. Consequently, it can be compressed to a relatively small size. On the other hand, high entropy images such as an image of heavily cratered areas on the moon have a great deal of contrast from one pixel to the next and consequently cannot be compressed as much as low entropy images.

2.6.5.1. Calculating Image Entropy

Image entropy, as used in my compression tests, is calculated with the same formula used by the Galileo Imaging Team:

\[
Entropy = - \sum_{i=1}^{255} P_i \log_2 P_i
\]

(2.7)
In the last expression, $P_i$ is the probability that the difference between 2 adjacent pixels is equal to $i$, and $\log_2$ is the base 2 logarithms.

2.6.6. Similarity Metrics

Metrics are probably the most critical elements of a registration problem. The metrics define what the goal of the process is. They measure how well the Target object is matched by the Reference object after the transform has been applied to it. The Metric should be selected in function of the types of objects to be registered and the expected kind of misalignment. Some metrics have a rather large capture region, which means that the optimizer will be able to find his way to a maximum even if the misalignment is high. Typically large capture regions are associated with low precision of the maximum. Other metrics can provide high precision for the final registration, but usually require to be initialized quite close to the optimal value. Unfortunately, there are no clear rules about how to select a metric but some of them can be tried in different conditions. In some cases, it could be an advantage to use a particular metric to get an initial approximation of the transformation, and then switch to another more sensitive metric to achieve better precision in the final result.
2.7. Soft Computing Algorithms

Soft computing is an important branch of study in the area of intelligent systems and based knowledge. It has effectively complemented conventional artificial intelligent (AI) in the area of machine intelligence. Soft computing can be defined as the use of inexact solutions to computationally hard tasks such as the solution of nondeterministic polynomial time (NP) complete problems. It is referred to the science of dialectics, deduction and thinking that recognizes and uses the real world phenomena of grouping, classification and memberships of various quantities under study. In real world, we have many problems which we have no way to solve logically, or problems which could be solved theoretically but actually impossible due to its requirement of huge resources and huge time required for computation. For these problems, methods motivated by nature sometimes work very efficiently and effectively. Although the solutions obtained by these methods do not always equal to the mathematically strict solutions, a near optimal solution is sometimes enough in most practical purposes. These biologically inspired methods are called Soft Computing. [39] Genetic algorithm, Fuzzy logic, Neural Networks and Probability Theory are used in soft computing for knowledge representation and for mimicking the reasoning and decision-making processes of a human. Quite effective are the mixed or hybrid techniques, which synergistically exploit the advantages of two or more of these areas. [40] Decision making with soft computing involves approximate reasoning. In this chapter will give an introduction to the subject of soft computing, with an emphasis on fuzzy logic and genetic algorithms. The tools of soft computing and its application will be covered in this chapter. Soft computing is a wide ranging group of techniques such as neural networks, genetic algorithms, nearest neighbor, particle swarm optimization, ant colony optimization, fuzzy systems, rough sets, simulated annealing, DNA computing, Quantum computing, Membrane computing etc. While some of these techniques are still in the emerging stage, the rest of them have found wide spread use in the area of Pattern recognition, Classification, Image processing, Voice recognition, Data mining etc. Each of these methodologies has their own strength. The seamless integration of these methodologies to create intelligent systems forms the core of soft computing. [41]
Soft Computing is useful where the precise scientific tools are incapable of giving low cost, analytic, and complete solution. Scientific methods of previous centuries could model, and precisely analyze, merely, relatively simple systems of physics, classical Newtonian mechanics, and engineering. Soft computing is a collection of methodologies, which in one form or another reflect the guiding principle of soft computing: exploit the tolerance for imprecision, uncertainty, and partial truth to achieve tractability, robustness, and low solution cost. Viewed in a slightly different perspective, soft computing is a consortium of methodologies which, either singly or in combination, serve to provide effective tools for the development of intelligent systems [42].

2.7.1. Soft Computing Tools

In this section displayed a briefly outline some of the common soft computing tools (Neural Network, Genetic Algorithm and Fuzzy Logic) based on their fundamental characteristics.

2.7.1.1. Artificial Neural Network

An ANN is a parallel distributed information processing structure consisting of a number of nonlinear processing units called neurons. The neuron operates as a mathematical processor performing specific mathematical operations on its inputs to generate an output. [43] It can be trained to recognize patterns and to identify incomplete patterns by resembling the human-brain processes of recognizing information, burying noise literally and retrieving information correctly. In terms of modeling, remarkable progress has been made in the last few decades to improve ANN. ANN are strongly interconnected systems of so called neurons which have simple behavior, but when connected they can solve complex problems. Changes may be made further to enhance its performance. [44]
2.7.1.2. Genetic Algorithms

Evolutionary algorithms (EA) were invented to mimic some of the processes observed in natural evolution. Evolution occurs on chromosomes - organic devices for encoding the structure of living beings. Processes of natural selection then drive those chromosomes that encode successful structures to reproduce more frequent than those that encode failed structures. In other word, the chromosomes with the best evaluations tend to reproduce more often than those with bad evaluations. By using simple encodings and reproduction mechanisms, the algorithms can then display complicated behavior and turn out to solve some extremely difficult problems [45].

GAs are a special subclass of a wider set of EA techniques. GA were named and introduced by John Holland in the mid-1960s. Then Lawrence Fogel began to work on evolutionary programming and Ingo Rechenberg and Hans-Paul Schwefel introduced the evolution strategy. In resolving difficult problems where little is known, their pioneered work stimulated the development of a broad class of optimization methods [46]. Subsequently the genetic algorithms were studied by De Jong and Goldberg. Others such as Davis, Eshelman, Forrest, Grefenstette, Koza, Mitchell, Riolo, and Schaffer, to name only a few, GA had been most frequently applied to the domain of optimization [47]. Based on the principles of natural evolution, GAs are robust and adaptive methods to solve search and optimization problems [48]. Because of the robustness of genetic algorithms, a vast interest had been attracted among the researchers all over the world [49]. In addition, by simulating some features of biological evolution, GA can solve problems where traditional search and optimization methods are less effective. Therefore, genetic algorithms have been demonstrated to be promising techniques which have been applied to a broad range of application are as [50]. The ability to apply GA to real-world problems has improved significantly over the past decade [45].
2.7.1.3. Fuzzy Logic

In the real world, information is often ambiguous or imprecise. When we state that it is warm today, the context is necessary to approximate the temperature. A warm day in January may be degrees Celsius, but a warm day in August may be 33 degrees. After a long spell of frigid days, we may call a milder but still chilly day relatively warm. Human reasoning filters and interprets information in order to arrive at conclusions or to dismiss it as inconclusive. Although machines cannot yet handle imprecise information in the same ways that humans do, computer programs with fuzzy logic are becoming quite useful when the sheer volume of tasks defines human analysis and action. An organized method for dealing with imprecise data is called fuzzy logic. The data sets engaged in fuzzy logic are considered as fuzzy sets. Traditional sets include or do not include an individual element; there is no other case than true or false. Fuzzy sets allow partial membership. Fuzzy Logic is basically a multi-valued logic that allows intermediate values to be defined between conventional evaluations like yes/no, true/false, black/white, etc. Notions like rather warm or pretty cold can be formulated mathematically and processed with the computer. In this way, an attempt is made to apply a more humanlike way of thinking in the programming of computers. Fuzzy logic is an extension of the classical propositional and predicate logic that rests on the principles of the binary truth functionality. Fuzzy logic is a multi-valued logic. However, the most pertinent feature of fuzzy logic for which it receives so much attention is its scope of partial matching. In any real world system, the inferences guided by a number of rules follow a middle decision trajectory over time. This particular behavior of following a middle decision trajectory [51] is human like and is a unique feature of fuzzy logic, which made it so attractive. Very recently, Prof. Zadeh highlighted another important characteristic [52] of fuzzy logic that can distinguish it from other multivalued logics. He called it f.g-generalization. According to him any theory, method, technique or problem can be fuzzified (or f-generalized) by replacing the concept of a crisp set with a fuzzy set. Further, any theory, technique, method or problem can be granulated (or g-generalized) by partitioning its variables, functions and relations into granules (information cluster). Finally, we can combine f-generalization with generalization and call it f.g-generalization. Thus ungrouping an information system into components by some strategy and regrouping them into
clusters by some other strategy can give rise to a new kind of information sub-
systems. Determining the strategies for ungrouping and grouping, however, rests on
the designer’s choice. The philosophy of f.g generalization undoubtedly will re-
discover fuzzy logic in a new form.

2.7.2. Application Areas of Soft Computing

Soft computing techniques have become one of promising tools that can provide
practice and reasonable solution. Soft computing techniques are used in different
fields: [39]

2.7.2.1. Computer Engineering

Computer engineering is a subject that included several fields of computer science
and electrical engineering required to develop computer systems. Computer engineers
commonly have training in software design, hardware-software and electronic
engineering integration instead of only software engineering or electronic
engineering. Computer engineers are engaged in many software and hardware aspects
of computing, from the design of individual microprocessors, personal computers and
supercomputers to circuit design. The engineering field not only focuses on the
working of computer systems themselves, but also how they integrate into the larger
picture.

2.7.2.2. Feature Selection

In machine learning and statistics the feature selection is the process of selecting a
subset of relevant features for use in model construction. Feature selection techniques
are a subset of the more general field of feature extraction. Feature extraction creates
new features from functions of the original features, whereas feature selection returns
a subset of the features. [39]

2.7.2.3. Medical diagnosis

Medical diagnosis refers to the process of attempting and the opinion reached by
this process to determine or identify a possible disease. From the point of view of
statistics the diagnostic procedure involves classification tests.
2.7.2.4. Image Processing

In imaging science the image processing is any form of signal processing for which the input is an image such as a photograph or video frame and the output of image processing may be either an image, a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal processing techniques to it. [53]

2.7.2.5. Industrial Machineries

Industries machineries are tools that consist of one or more parts, which are uses energy to achieve a particular goal. Usually they are powered by mechanical, thermal, chemical or electrical means, and are frequently motorized. This is used in mechanical engineering.

2.7.2.6. Process Control

Process control is a statistics and engineering discipline that deals with architectures, mechanisms and algorithms for preserving the output of a specific process within a desired range. It is extensively used in industry and enables mass production of continuous processes such as power plants, paper manufacturing, oil refining, chemicals and many other industries. Process control enables automation to operate a complex process from a central control room with a small staff of operating personnel.

2.7.2.7. Smart Instrumentation

As intelligent devices become widespread the challenge is to connect sensors and actuators through smart systems. A main issue is the increasing number of communication protocols, with no single standard. The challenge is to intelligently connect smart instrumentation so that devices can communicate across multiple protocols. At the same time, increases in the volume and importance of data means that privacy, security and robustness of systems is paramount.
2.7.2.8. Pattern Recognition

The aim of pattern recognition is to provide a reasonable answer for all possible inputs and to perform “most likely” matching of the inputs taking into account their statistical variation. Pattern recognition is studied in different fields such as computer science, cognitive science, traffic flow, psychology, psychiatry and ethology.

2.7.3. Image Encryption Using Soft Computing Algorithms

Soft Computing is an emerging field that consists of complementary elements of fuzzy logic, neural computing and evolutionary computation. Soft computing techniques have found wide applications. One of the most important applications is image security. In this section, the main aim is to survey the theory of image security using soft computing approach based on the Fuzzy logic and Genetic Algorithm. As digital information transmissions are increased, the problem of protecting data from illegal access has become a challenging task. In order to fulfill such a task, many image encryption methods have been proposed in the past. However some of them have been known to be insecure. As images form a main source of conveying information, novel encryption techniques are needed for secured transfer of information. Traditional data encryption techniques can be divided into two categories namely substitution and transposition, which are used individually or in combination in every cryptographic algorithm. In substitution technique, one symbol in the data is replaced by another symbol according to some algorithm. In transposition technique, positions of symbols are reordered according to some rule. The genetic algorithm is based on both substitution and transposition operations. It works on the basis of Darwinian evolution theory. Genetic operation is divided into three steps: selection, crossover and mutation. The crossover process works like transposition and mutation like substitution technique.
2.8. Literature Review on Image Encryption

- **Image Encryption Based on Chaos Theory and Chaotic Map**
  A chaos-based image encryption schemes typically consist of iteration of two processes (i) permutation and (ii) diffusion. The permutation is achieved by scrambling all the pixels as a whole using 2D chaotic map (such as Baker map, Arnold cat map etc. [54-58]. During diffusion, the pixel values are modified sequentially and the change made to a particular pixel depends on the accumulated effect of all the previous pixel values. However, as many rounds of permutation and diffusion or iterations should be taken, the overall encryption speed is slow.

- **Chaos-Based Random Number Generator**
  For a truly random generator, the number of ones and zeros in the output are equal. It is possible to formulate many other statistical properties that describe the key stream generated by a random source. Various test suites are available in the literature. These statistical tests are designed to evaluate the randomness properties of a finite sequence. The chaotic orbit generated by a nonlinear system is irregular, a periodic, unpredictable, and has sensitive dependence on the initial conditions. These characteristics coincide with the confusion and diffusion properties in cryptography. Therefore, in recent years, the chaotic system has been studied for security in both analogue and digital forms.
  Chen et al (2010) suggested a nonlinear Digitalized Modified Logistic Map-based Pseudo Random Number Generator (DMLM-PRNG) for enhancing randomness. Two techniques, i.e., constant parameter selection and output sequence scrambling are employed to reduce the computation cost, without sacrificing the complexity of the output sequence. [59] Chaotic map-based PRNGs have been proposed by Addabbo et al 2007 and Callegari et al (2005).
  Savi (2007) considered randomness as fluctuations and uncertainties due to noise and investigated its influence on the nonlinear dynamic behaviour of coupled logistic maps. The noise effect is included by adding random variations, either to the parameters or to the state variables. [60]
Chang et al (2007) introduced a robust chaotic map. The modified logistic map, which not only exhibits no chaotic window but also uniformly distributes in 0, 1. On the basis of this map, they designed a multi-system hyper-chaotic synchronization, an asymptotic synchronization of the modified logistic hyper-chaotic system for secure communication. It can theoretically achieve asymptotical synchronization between the transmitter and receiver after finite times in simplex partial coupling transmission. Furthermore, the implicit driving technique always guarantees asymptotical synchronization between the drive and response systems during plain text transmission.[61]

Rani and Agarwal (2009) established new method to enhance the capabilities of the logistic map via superior iterations. Logistic transformations $x_{n+1} = rx_n(1 - x_n)$ for choosing $x_0$ between 0 and 1 and $0 < r_4$. Where $x_n$ lies between zero and one, and represents the population at year n. Therefore, $x_0$ represents the initial population (at year 0) and $r$ represents a positive combined rate for reproduction and starvation. They have found a celebrated place in chaos, fractals and discrete dynamics. The stability of logistic map is studied by running computer programs. The logistic map is stable for $0 < r \leq 3.2$ in Picard orbit. In superior orbit, the range of stability of the logistic map increases drastically. Also, the behaviour of the map disappears in certain cases. [62]

- **Stream Encryption Scheme**

Stream encryptions are based on generating an infinite cryptographic key stream, and are used to encrypt one bit or byte at a time. Stream ciphers have relatively low memory requirements. This section gives a brief review on stream encryption schemes.

Chen et al (2004) proposed a symmetric image encryption scheme based on 3D chaotic cat maps. The two-dimensional chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption scheme. This scheme employs the 3D cat map to shuffle the positions of image pixels, and uses another chaotic map to confuse the relationship between the cipher-image and the plain-image, thereby significantly increasing the resistance to statistical and differential attacks. [63]
A new gray-level image encryption scheme based on phase encoded exclusive (XOR) operations and a full phase encoding method are implemented by Shin et al (2004). The gray-level image can be sliced into binary images which have the same pixel level, and each of them is encrypted by phase-encoded XOR operations with each phase-encoded binary random image. They combine XORed images and phase-encoded binary random images into an encrypted image and a key image, respectively. Gray-level encrypted data and key data are obtained by the phase-encoding process of the encrypted image and the key image in a space domain. [64]

Zhang et al (2005) proposed an image encryption approach based on chaotic maps, to improve the properties of confusion and diffusion in terms of discrete exponential chaotic maps, and designed a scheme for resisting statistic, differential and grey code attacks. [65]

Wong et al (2008) designed a new scheme to introduce certain diffusion effect in the substitution stage by simple sequential add-and-shift operations. Although this leads to a longer processing time in a single round, the overall encryption time is reduced as fewer rounds are required. [66]

Mazloom and Eftekhar-Moghadam (2009) proposed a Coupled Nonlinear Chaotic Map (CNCM), based on image encryption algorithm, to encrypt colour images using CNCM. The chaotic cryptography technique is used as a symmetric key cryptography with a stream cipher structure. In order to increase the security of the proposed algorithm, 240 bit-long secret key is used to generate the initial conditions and parameters of the chaotic map by making some algebraic transformations to the key. These transformations as well as the nonlinearity and coupling structure of the CNCM have enhanced the cryptosystem security. [67]

Wang et al (2009) proposed chaos-based image encryption algorithm with variable control parameters. The control parameters used in the permutation stage and the key stream employed in the diffusion stage are generated from two chaotic maps related to the plain-image. As a result, the algorithm can effectively resist all known attacks against permutation diffusion architectures. [68]

The cryptosystem employing two-dimensional chaotic maps for document encryption is suggested by Xiang et al (2007). Several widely used two-dimensional chaotic maps are considered and their performances are investigated. [69]
Yoon and Kim (2010) proposed an image encryption algorithm using a large pseudo random permutation which is combinatorially generated from small permutation matrices based on chaotic maps. The random-like nature of chaos is effectively spread into encrypted images by using the permutation matrix. [70] 

Akhshani et al (2010) designed a new scheme for two-dimensional piecewise nonlinear chaotic maps with an invariant measure and then used to design a fast and highly secure symmetric image encryption scheme. These maps have advantages such as invariant measure, ergodicity and the possibility of K-S entropy calculation. In this scheme, its control parameters and initial values can all be used as encryption key in chaotic cryptosystem. [71] 

Ye (2010) introduced an image scrambling encryption algorithm of pixel based on chaos map. The algorithm uses a single chaos map only once to implement the gray scrambling encryption of an image, in which the pixel values ranging from 0 to 255 are distributed evenly; the positions of all pixels are also permutated. In this way, the proposed method transforms drastically the statistical characteristic of original image information and so it increases the difficulty of an unauthorized individual to break the encryption. [72] 

A robust image encryption method by using the integral imaging and Pixel Scrambling (PS) techniques is proposed by Piao et al (2009). In this method, pixels of the colour image are scrambled with the PS technique and elemental images for this scrambled image are picked up through a lenslet array. Subsequently, an encrypted image is obtained by scrambling these picked-up elemental images. Since this encrypted image has the hologram like property of data redundancy resulted from the integral imaging scheme, it can as well be decoded by multiple keys such as the orders of pixel scrambling. [73] 

Sun et al (2010) designed a new cryptosystem based on Spatial Chaos System (SCS), which is investigated by conducting FIPS 140-1 statistic test, and is especially useful for encryption of digital images. It is shows how to adapt a two dimensional ergodic matrix obtained from SCS to permute the positions of image pixels and confuse the relationship between the cipher-image and plain-image simultaneously. [74] 

Kumar and Ghose (2011) proposed an extended substitution diffusion based image cipher using chaotic standard map and linear feedback shift register. The first stage
Encryption and Decryption Image Using Multiobjective Soft Computing Algorithm

consists of row and column rotation and permutation which is controlled by the pseudo random sequences which is generated by standard chaotic map and linear feedback shift register. In the second stage, further diffusion and confusion are obtained in the horizontal and vertical pixels by mixing the properties of the horizontally and vertically adjacent pixels respectively with the help of chaotic standard map. The number of rounds in both stages is controlled by combination of pseudo random sequence and original image. [75]
Zhang and Liu (2011) proposed a novel image encryption method based on skew tent chaotic map and permutation-diffusion architecture. In this proposed method, the P-box is chosen as the same size of plain-image, which shuffles the positions of pixels totally. The key stream generated by skew tent chaotic map is related to the plain-image. There has been a large amount of research in stream based encryption, as well. [76]

• Block Encryption Scheme
Block encryption is an encryption scheme in which the plain text is broken up into blocks of fixed length and encrypted one block at a time. Block ciphers can provide integrity protection and confidentiality. Chaotic block ciphers transform blocks by directly applying the chaotic maps. This section gives a brief review of block encryption schemes.

Amin et al (2010) proposed a chaotic block cipher scheme for image cryptosystems that encrypts block of bits rather than block of pixels. It encrypts 256-bits of plain-image to 256-bits of cipher-image within eight 32-bit registers. The scheme employs the cryptographic primitive operations and a nonlinear transformation function within encryption operation and adopts round keys for encryption using a chaotic system.[77]
A block cryptographic scheme based on iterating a chaotic map is presented by Xiang et al (2006). With random binary sequences generated from the real-valued chaotic map. The plain text block is permuted by a key dependent on shift approach and then encrypted by the classical chaotic masking technique. [78]
Kwok and Tang introduced a fast chaos based image encryption system with stream cipher structure to achieve a fast throughput and to facilitate hardware realization. Further a 32-bit precision representation with fixed point arithmetic is assumed. The major core of the encryption system is a pseudo random key stream generator based on a cascade of chaotic maps, serving the purpose of sequence generation and random mixing. Unlike the other existing chaos based pseudo-random number generators, the proposed key stream generator not only achieves a very fast throughput, but also passes the statistical tests of up-to-date test suite even under quantization. [79]

A fast image encryption and authentication scheme is stated by Yang et al (2010). In particular, a keyed hash function is introduced to generate a 128-bit hash value from both the plain-image and the secret hash keys. The hash value plays the role of the key for encryption and decryption while the secret hash keys are used to authenticate the decrypted image. [80]

A block encryption for image using combination of confusion and diffusion is suggested by Wang et al (2010). Baker map is used to generate a pseudo-random sequence, and several one-dimension chaotic maps are dynamically selected to encrypt blocks of image. When diffusion is executing, for mutual diffusion of pixels, the confusion is working by the pseudo random order of route and the combination is deep seated.[81]

A block encryption scheme based on dynamic substitution boxes (S-boxes) is considered by Wang et al (2009). The difference trait of the tent map is analyzed. Then, a method for generating S-boxes based on iterating the tent map is presented. The plain texts are divided into blocks and encrypted with different S-boxes. The cipher blocks are obtained by 32 rounds of substitution and left cyclic shift.[82]

Wang et al (2011) introduced a fast image encryption algorithm with combined permutation and diffusion. First, the image is partitioned into blocks of pixels. Then, spatiotemporal chaos is employed to shuffle the blocks and at the same time, to change the pixel values. Meanwhile, an efficient method for generating pseudo random numbers from spatiotemporal chaos is suggested, which further increases the encryption speed. [83]
Awad (2011) presented a robust chaos-based cryptosystem for secure transmitted images and four other versions. In the proposed block encryption/decryption algorithm, a 2D chaotic map is used to shuffle the image pixel positions. Then, substitution and permutation operations on every block, with multiple rounds, are combined using two perturbed chaotic maps. Therefore, the block encryption scheme has been considered as one of the most important topics in encryption, by many researchers.[84]

❖ Scrambling Algorithm

• Sign Scrambling Algorithm
  Shi and Bhargava(1998 -1999) implemented a new method to encrypt the sign bit of every (Discrete Cosine Transform) DCT coefficient in JPEG [85] and every motion vector in MPEG [86]. This approach is really fast and easy to implement. It is robust to the compression because the sign bit is not changing with respect to different quantization tables. However it lacks security and affects compression efficiency as a result of encrypting DCT coefficients before run-length and Huffman coding. Since the sign bit could be viewed as the most significant bit of coefficients, the results of the sign encryption expected to be good. The experiments in [85] and [86] show that the image/video would be totally unrecognizable after sign bits are randomly altered. To see the results of the sign encryption algorithm, it is implemented on MATLAB. Sign encryption is applied to Lena image with 8x8 logical scrambling matrixes, which could only take 0 or 1 as a value. The results are not good as it is expected. Therefore, selectively encrypting sign bit of every DCT coefficient is not an effective way for image/video encryption. But, because of simplicity, it can be used with other encryption methods for higher security level.

• Slice Scrambling
  It is another approach for image encryption. Wu and Kuo (2003) mentioned an encryption algorithm, which scrambles equal size of 8x8 DCT blocks with respect to a table No. 1 in [87]. This approach is also easy to implement and robust to the compression, since different quantization tables will only change coefficients of the block but not the arrangement of the blocks. However, it affects the compression
efficiency because of placing uncorrelated DC coefficients next to each other and lacks security since one can change the block arrangement with respect to the correlation of the blocks. Moreover, the block arrangement permutation should be embedded to the key, which makes key sizes very high in small block cases. The contour is recognizable in the encrypted image when block size is large. It doesn’t seem very secure even visually. Moreover, the key size gets larger with small block sizes. On the other hand, the inner blocks are not encrypted. Therefore, the correlations of the originally near blocks are high. This information can be used to reconstruct original image. As a result, this method also can’t be used in practice.

- **DCT Coefficient Scrambling**

  Tang (1996) suggested shuffling the DCT coefficients within an 8x8 block for JPEG/MPEG based transmission system [88]. This technique is fast and simple to implement. However, it changes the statistical property (run-length characteristic) of DCT coefficients. As a result, it may increase the bitrate drastically. But it lacks security. No contour is recognizable in the encrypted image. Visually, it is very secure, but since only inner blocks are encrypted, it has been shown in [89] that this chipper is vulnerable to frequency-based attack that exploits the property of none-zero coefficients that have the tendency to appear earlier in the zigzag order. In addition, it may increase the bitrate of the compressed video by as much as 50% as reported in [88] and this approach also may not be amenable to secure bitrate conversion. Therefore, this method also can’t be used in practice.

- **Line Scrambling**

  There are several video scrambling systems [90, 91] which rely on methods of directly distorting the image in the spatial domain. These scrambling techniques are not efficient for transmitting digital video signals because they, in general, will significantly chance the statistical property of the original video signal [87]. One of the spatial domain scrambling approaches is line scrambling which scrambles the lines of the image to experiment spatial domain scrambling effects, line scrambling algorithm is implemented on MATLAB. A permutation of the sequence from 1 to image height is used to rearrange the image lines No contour is
recognizable in the encrypted image. Visually it is very secure. But the file size of the scrambled image is 30% more than original. Therefore, using of this method is not proper for the limited bandwidth systems.

**Image Encryption Based on Transforms**

- **Fourier Transforms**
  Ran Tao et al (2010) introduced another technique for image encryption using multi-order fractional Fourier transform. In this technique, the encrypted image is obtained by the summation of different orders of Inverse Discrete Fractional Fourier Transform (IDFR FT) of the interpolated sub-images. The whole transform orders of the utilized FFT are used as the secret keys for the decryption of each sub-image. Compared with the traditional image encryption methods based on the FRFT, the method is with a larger key space and the amount of keys can be set as large as two times the amount of the pixels in the original image. In future work, one can also combine the proposed method with other image encryption methods to enhance the security of the system [92].
  Zhengjun Liu et al (2011) proposed an image encryption algorithm based on fractional Fourier transform. A local random phase encoding is introduced into this algorithm. The data at the local area of complex function is converted by fractional Fourier transform [93].

- **Wavelet Transform**
  Zhu Yu et al (2010) proposed Chaos-Based image encryption algorithm using Wavelet Transform. Algorithm uses the wavelet decomposition concentrating image information in the high-frequency sub-band and then encryption is applied for the sub-band image. After that a wavelet reconstruction is introduced in order to spread the encrypted part throughout the whole image. A second encryption process is used to complete the encryption process. Theoretical analysis and experimental results show that this algorithm has an obvious increase in efficiency as well as satisfied security [94].
Image Encryption Using Soft Computing Algorithm

- Genetic Algorithm

Ankita Agarwal (2012) established a new approach of Genetic Algorithm in which the operations of GA (Crossover and Mutation) are used to produce this encryption method. This new method was applied to the candidate’s type of data i.e. images. [95]

Sandeep Bhowmik(2011) tried to analyze the application of GA for image security using a combination of block-based image transformation and encryption techniques. The cases show that the correlation among pixels decreased when the proposed algorithm was applied to images [96].

Jalesh Kumar and S. Nirmala (2012) implemented a new technique to encrypt image, which utilizes selection crossover and mutation operations. This technique based on genetic algorithm, comprises three stages; the first stage deals with the selection of key sequence. In this stage, linear congruential pseudo random generator is used for generating key sequence. The second stage is deals with the crossover operation. The third stage deals with the mutation operation on the result obtained from the previous stage. This method combines transposition and substitution methods to encrypt the data. [97]

Aarti Soni and Suyash Agrawal (2013) presented a new method based on genetic algorithm which is used to generate a key by the help of pseudo random number generator. Random number will be generated on the basis of current time of the system. Using Genetic Algorithm can keep the strength of the key good and make the whole algorithm good enough. Symmetric key algorithm AES has been proposed for encrypting the image as it is very secure method for symmetric key encryption. This algorithm increased the efficiency of the algorithm in terms of computation time required and complexity to attack the message. It uses the concept of pseudo random number generator and genetic algorithms to increase the complexity of key by increasing the irregularity of the key. Implementation of Genetic Algorithm with PRNG has a very complex key which is very difficult for cryptanalyst to attack. The AES symmetric key encryption algorithm will provide an efficient method for encrypting image and increasing the overall efficiency of the system [98].
Abdelsalam et al (2010) propose a new approach for e-security applications using the concept of genetic algorithms with pseudorandom sequence to encrypt and decrypt data stream. The feature of such an approach includes high data security and high feasibility for easy integration with commercial multimedia transmission applications. An experiment testing feasibility is reported in which several images are encrypted and decrypted. The experimental results show that the proposed technique achieved high throughput rate that is fast enough for real time data protection. In this technique used the concept of genetic algorithms in cryptography along with the randomness properties of Non-Linear Feedback Function Shift Register (NLFFSR). This total way of transferring secret information is highly safe and reliable. So, without the knowledge of the pseudorandom sequence no one will be able to extract the message. Since the NLFFSR pseudorandom binary sequence is unpredictable it is very difficult to decrypt correctly an encrypted signal by making an exhaustive search without knowing the initial value and the feedback function $f$ and non linear output function. [99]

Srikanth et al (2010) suggested a new algorithm to encrypt an image by using genetic algorithm. In this algorithm first the image is broken down into blocks Then the initial transformation steps are performed after that the functions similar to Vernon cipher are used to locate the pixels and further genetic algorithm is used to encrypt the images using one point cross-over. This algorithm can be classified as comparatively, more efficient and less complex when it is compared to the existing spatial domain techniques. [100]

Ahmed Mahamood et al (2013) presented a novel efficient symmetric encryption technique which can be applied to medical images. It uses genetic algorithm to become highly adaptive. Standard Digital Imaging and Communications in Medicine (DICOM) images are segmented into number of blocks based on pixels intensity and entropy measurements. The novelty of this technique is variable key length which controls the relationship between processing time and resulting robustness. Using an evolutionary based technique in the form of genetic algorithms creates an adaptive optimized method that controls the processing time by applying five adjusting parameters. These parameters are: encryption algorithms, key-length, robustness parameter (CORR, NPCR), number of regions, and side information. [101]
Dr. Dilbag et al (2013) designed a new algorithm using the concept of genetic algorithms. This algorithm enhances the quality, efficiency and effectiveness of the algorithm by using cryptography. Genetic algorithms are used to find an optimized solution within minimum possible time. [102]

- **Fuzzy Sets Theory**

  Said E. El-Khamy et al (2005) introduced a new colour image encryption system. This system uses a Fuzzy Bit Generator (FBG) which was developed by the researcher. Moreover by using a fuzzy PN bit generator generated four binary sequences which are used to encrypt image pixels. According to these sequences, each pixel colour byte value rotated as bits in right or left direction for some bits, after rotation process the pixel colour XOR-ed by one of binary sequences. According to image dimensions, the bits of $S_0, S_1$ are used to get the coordinate of the upper left corner of a 4x4 pixel blocks $B_i$ of the image under encryption $x_i$ and $y_i$. $S_2, S_3$ are used to get the coordinates $x_{i+1}$ and $y_{i+1}$ for $B_{i+1}$. Having these randomly chosen blocks, the variance $\sigma_i^2$ and $\sigma_{i+1}^2$ are calculated. The value of the variance was used in the permutation scheme. [103]

Srinivasa et al (2012) proved a fuzzy logic method to fuse images from different sensors, in order to enhance the quality of proposed method. Along with quality evaluation parameters: image quality index (IQI), mutual information measure (MIM), root mean square error (RMSE), peak signal to noise ratio (PSNR), fusion factor (FF), fusion symmetry (FS) and fusion index (FI) and entropy. In this method, the potentials of pixel level image fusion using fuzzy logic approach have been explored along with quality evaluating measures. Fused images are primarily used to human observers for viewing or interpretation, and to be further processed by a computer using different image processing techniques [104].

Maneckshaw and Krishna Kumar (2013) proposed a novel Image encryption algorithm based on multiple fuzzy graph (FG) mapping technique. The Fuzzy graphs are obtained from a matrix of size $n$ and then they are used to encrypt an image. They are discussed the fuzzy graphs with triangular and sigmoid membership functions.
They are obtained a desired graph with the help of sigmoid function from a matrix by considering the vertices as the entries of the matrix and connecting edges between them whenever they are adjacent. To encrypt the image using the technique of multiple FG mapping, they are undergo the process of image encryption by dividing it into three stages – shuffling, mapping and encryption in order to have a greater security levels. This method has a larger key space, i.e., the randomly obtained pixel values which are combined with the pixels of the original image. These pixels are influenced by the factors such as the chosen matrix, the size of the matrix, the types of graphs obtained, the types of membership functions chosen, the patterns of fuzzy graphs obtained and the blocks they are plotted. This technique provides a multiple levels of securities for the image encryption. [105].

ShreyamshaKumar and Chidamber Patil (2010) designed a new scheme for encrypt JPEG image. In the designed scheme the modified DCT blocks are confused by a fuzzy PN sequence. In addition to that, the DCT coefficients of each modified DCT block are converted to unique uncorrelated symbols, which are confused by another fuzzy PN sequence. Finally, the variable length encoded bits are encrypted by chaotic stream cipher. An amalgamation of all the three techniques with random combination of seeds will provide the required security against the casual listener/observer where the security needed is only in-terms of few hours. An image encryption algorithm that works co-operatively with JPEG compression has been proposed to meet three major requirements: (i) to provide temporal security against casual observer, (ii) to preserve the compression ratio, (iii) remain compliant with the JPEG file format. The experimental results of this scheme show that the encryption scheme provides the required security along with JPEG compression. Further, it preserves the compression ratio and the JPEG file format. All these advantages make it suitable for secure image coding and tactical communication. [106]
Encryption and Decryption Image Using Multiobjective Soft Computing Algorithm

- **Neural Networks**

  Hüsamettin UYSAL and Sinem KURT (2012) designed automatic system based on artificial neural networks for decrypting an image automatically without knowing what the decoder. In this study, decryption through MLP (Multilayer Perceptron) and RBF (Radial Basis Function) networks was tested using the interface which was designed in Matlab GUI and the image was shown and saved with minimum error by calculating the error rates of decrypted images. They are determined the differences between RBF and MLP. RBF was better than MLP with shorter processing time and less error rate. The main difference of this study from other related ones is using ANN for encoding and decoding. The procedure of this system consists of decoding the encrypted images by ANN to obtaining the original image. As a result, it is succeeded to obtain almost the same image of the original image easily by ANN. [107]

Ismail I. A. et al (2012) proposed an algorithm to encrypt and decrypt satellite image by using neural networks back propagation. The goal of proposed algorithm to investigate the applicability of a back-propagation artificial neural network on the encryption of huge-sized satellite images. The used network is of $N \times M \times N$ neurons representing the input, hidden, and output layers, respectively. The network is trained by adjusting the weights while the bias is given a constant value between 0 and 1 after normalizing the values. A bias is determined. The bias between the input layer and the hidden layer works as the first key ($K_1$), while the bias between the hidden layer and the output layer represents a second key ($K_2$). The training method uses $K_1$, $K_2$, or both and is done using images of small sizes to improve speed. Then, the network is used to encrypt and decrypt normal satellite images. Numerous trials were done for different satellite optical and SAR images and the goodness of fit (quality of decryption) between the original images and the decrypted ones was at least 98%, even for the images that the network was not previously trained to decrypt. It was also found that the network is not affected by geometrical image distortions like translation, size, and rotation.[108]
• **Hybrid Algorithms**

Rasul Enayatifar and Abdul Hanan Abdullah proposed a new method based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. In their method, firstly, a number of encrypted images are constructed using the original image with the help of the chaotic function. Secondly, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Thirdly, the genetic algorithm is used to optimize the encrypted images as much as possible. Finally, the best cipher-image is chosen as the final image encryption [109]

Anil Kumar and Ghose M. K.(2009) proposed a new approach of genetic algorithms (GA) with pseudorandom sequence to encrypt data stream. For transmitting the secured data over the channel there is the requirement of the high throughput. In these cases, the conventional encryption techniques are not a feasible solution for this reason a high throughput and secure encryption technique is proposed for real time data transmission like over the telephone link or video transmission. The concept of Genetic Algorithms used along with the randomness properties of chaos. This total way of transferring secret information is highly safe and reliable. The simulation results have indicated that the encryption results are (1) completely chaotic by the sense of sight, (2) very sensitive to the parameter fluctuation. The experimental results of the proposed approach confirm that high throughput rate needed for real time data protection is achieved. [110]

Shubhangini et al (2013) suggested a novel method for image encryption by using chaotic function and genetic algorithm. This method, firstly images are encrypted using chaotic function and encryption key. Secondly genetic algorithm is used for optimization in which the best cipher image is selected. Finally the best cipher Images are selected based on correlation coefficient and entropy. [111]
Nooshin B. et al (2012) presented a novel image encryption/decryption algorithm based on chaotic neural network (CNN). The employed CNN is comprised of two 3-neuron layers called chaotic neuron layer (CNL) and permutation neuron layer (PNL). The values of three RGB (Red, Green and Blue) color components of image constitute inputs of the CNN and three encoded streams are the network outputs. CNL is a chaotic layer where, three well-known chaotic systems i.e. Chua, Lorenz and Lü systems participate in generating weights and biases matrices of this layer corresponding to each pixel RGB features. Besides, a chaotic tent map is employed as the activation function of this layer, and makes the relationship between the plain image and cipher image nonlinear. The output of CNL, i.e. the diffused information, is the input of PNL, where three-dimensional permutation is applied to the diffused information. The overall process is repeated several times to make the encryption process more robust and complex. A 160-bit-long authentication code has been used to generate the initial conditions and the parameters of the CNL and PNL. Some security analysis are given to demonstrate that the key space of the new algorithm is large enough to make brute-force attacks infeasible and simulations have been carried out with detailed numerical analysis, demonstrating the high security of the new image encryption scheme.[112]

Mouad et al (2011) presented a digital image encryption algorithm based on chaotic logistic maps and using fuzzy logic. The main idea of this algorithm is the usage of a fuzzy logic set of rules to control the next iteration of our proposed iterative mechanism using a set of logistic maps. The introduction of the fuzzy controller helped to use a set of logistic maps instead of one logistic map and therefore increased the randomness of the generated inputs. [113]

2.9. Conclusion

This chapter has given an overview of digital images and its formats, classification of encryption algorithm, basic concepts of image encryption, some measurements of image security, an overview of soft computing algorithms, its tools and applications and a literature review of image encryption