Introduction to Genetic Algorithm and Role in Image Processing

Kratika Giri Goswami[1] Dr. Anurag Paliwal[2]
[1]Research Scholar [2]Assistant Professor
[1,2]Geetanjali Institute of Technical Studies, Udaipur, India

Abstract— Genetic algorithm stimulate the process of biological evolution using survival principle of the fittest. Using genetic algorithm, digital image can be encrypted using different encryption techniques. In this each pixel of an image acts as an individual and these individuals are represented by a binary string which acts as chromosomes, then a group of chromosomes forms a population. After formation of population, random keys are generated using pseudorandom code which is used in encryption. The three main components of genetic algorithm are selection, crossover and mutation operator applied to the chromosome again and again.

Key words: Genetic Algorithm, Digital Image, Encryption, Random Keys, Pixels

I. INTRODUCTION

Genetic algorithms are new paradigms for adaptive agricultural search algorithms based on natural selection and the mechanism of natural genetics. They belong to the class of evolutionary algorithms to solve optimization problems that are used based on the mechanisms of biological evolution, such as mutation, intersection, selection and inheritance.

Genetic algorithm is the process of biological simulation of evolution, and through the intersection of the mutation. Genetic algorithms are blind optimization methods that do not need to be affected by the search space. Instead, they use payment values known as search ability. This quality may make genetic algorithm better than other local search procedures, such as gradient descent or greedy corrupt methods used for optimization. It was used for a variety of image processing programs, image

Segmentation, image compression, and extraction function of characteristics. The problem of developing images in this dissertation is an image segmentation. A technique used for mapping a region that represents an image.

II. PIXEL BASED FRAGMENTATION

Pixel-based methods specify local features such as borders and textures for extract areas of interest in images. The most common pixel-based operation is edge detector. Borders are defined as areas of the image with a high pixel density. Edge detection techniques use derivatives of first-class images, linear filtering techniques, the second Derivatives of the system to images. However, these techniques can produce broken edges and also include limits other features / details are in the image. Another method depends on the density is the area, starting from the seed point, Image cables and defragmentation by compiling a live pixel using similarities a standard such as the difference in the gray scale density values of two adjacent ones Pixels. The most complex features at the pixel level are the textures. The texture is generally defined in image processing is a region of pixels that are quantitatively related physical appearance of the surface. Formal fragmentation methods can be it is widely classified in methods of statistical, spectral and spatial filtering, based on the model methods. Statistical approaches such as time-based methods, co-occurrence matrices etc., and determine the textures, such as thickness, granular, smooth, etc. spectral and spatial the filtration methods try to simulate the human visual system through local performance.

III. DIGITAL IMAGE

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". 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 colors. 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. The pixel values in a binary image are any two values in general that are normalized, e.g., 0 and 1 or 0 and 255.

IV. ENCRYPTION AND DECRYPTION

Today, the Internet is moving towards multimedia data where the image covers the highest percentage. But with the growing growth of multimedia applications, security is an important aspect of communications and image storage, and encryption is a way to ensure security. The techniques of image encryption try to convert the original image into another image that is difficult to understand and maintain the confidentiality of the image among users. In other words, it is important to clarify that without a decryption key nobody can access the content. Images are widely used in many operations, so protecting images from unauthorized access is very important. Encryption is a data conversion to usable code over a public network. Encryption allows the sender to store sensitive information securely or transferred over non-secure networks so that they cannot be read by anyone except the recipient. Encrypting sensitive data is essential. It is used to make information incomprehensible if a transition is intercepted by unauthorized persons. It is called a clear form the normal (original) data / text information and image format is the concept of (protected data) and so-called text encryption / encryption image. It is called the normal text / image conversion process in the encrypted text / image encryption, while the conversion of text / reverse image encryption into the plain / text of the corresponding image is called the decryption process.

In general, most cryptographic algorithms use a secret value called a key. The security of the encrypted data depends entirely on two things: the strength of the encryption algorithm and the secretion of keys. It should be kept secret, which requires the sender and receiver to agree on the same

key before making any data transfer key used for encryption and decryption. The key is independent of plain text / normal image. Therefore, the same plain text / image is coded for different text / image codes with different keys. So both processes are impossible to complete without using the correct key. Encryption can be strong or weak. The encryption strength is measured by the time and resources you need to restore the normal / normal text image. The result of strong encryption is text encoding / imaging that is very difficult to decode without having the proper decryption tool. The sender and receiver must keep the key secret because anyone who knows the key can use it

V. ENCRYPTING AND DECRYPTING IMAGES USING A SOFT MULTI-COMPUTATION ALGORITHM

It is used to encrypt simple text / image in addition, the strength of the task algorithm. An unauthorized entity can take the encrypted text / encrypted image and seek to break the encryption by specifying the key based on the text / image codes. While encryption is the science of data security, cryptographic analysis is the science of analyzing and breaking down secure communications, so it is the process of restoring text / image or key, usually using text / code codes and knowledge of the algorithm.

Encryption can also be used to ensure the security of the communication path through:

1) Integrity of data means ensuring that data is not modified by unauthorized entities. Therefore, the message received by the receiver is the same as that sent by the sender.
2) Ensures that the issuer of any communication cannot deny its actions. This can be achieved through digital signatures along with asymmetric key encryption.
3) Authentication is the process of identification.
4) Privacy / confidentiality is the process of ensuring that no one can read the message, except to the intended recipient.

VI. PROPOSED METHOD

In this medical image processing pixels are considered corresponding to the chromosomes. Chromosomes are used to produce offspring's. Offspring will be the encoded form of an image.

A. Process of image encryption

1) Population Growth

In this process, a new set of population is generated from existing population by applying various sets of operation.

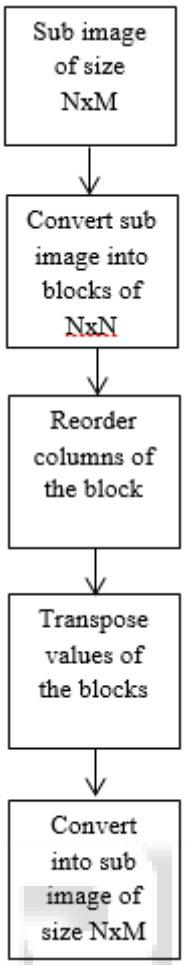

Fig. 1: Initial Population Growth

2) Crossover

In genetic algorithm, crossover is the process or genetic operator that is used to join two chromosomes. The newly generated chromosome is known as offspring which is replaced by the parent. This implies that there is no need for the selection operator as well as fitness function.

Chromosome 1	11011 00100110110
Chromosome 2	11011 1100011110
Offspring1	11011 1100011110
Offspring 2	11011 00100110110

Table 1: Crossover Process

3) Generation of key

Pseudorandom key is generated in the range of 1 to N using random number generator. The offspring produced acts as new set of chromosomes and are now crossover with generated keys.

For example two chromosomes (01011001 & 01110011) to be crossover using session key 11001011 and newly generated chromosomes are shown in the table.

Chromosome 1	01011001
Chromosome 2	01110011
Offspring1	01111001
Offspring 2	01010011

Table 2: Key Dependent crossover operation

4) Mutation process

Mutation randomly changes child from what's its parents produce in crossover. It is a genetic operator which changes

one or more bit in a chromosome. In this algorithm, swapping mutation is used.

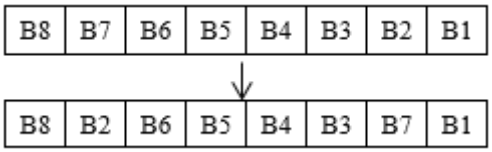

Fig. 2: Mutation Operation

5) Flowchart of Proposed Design

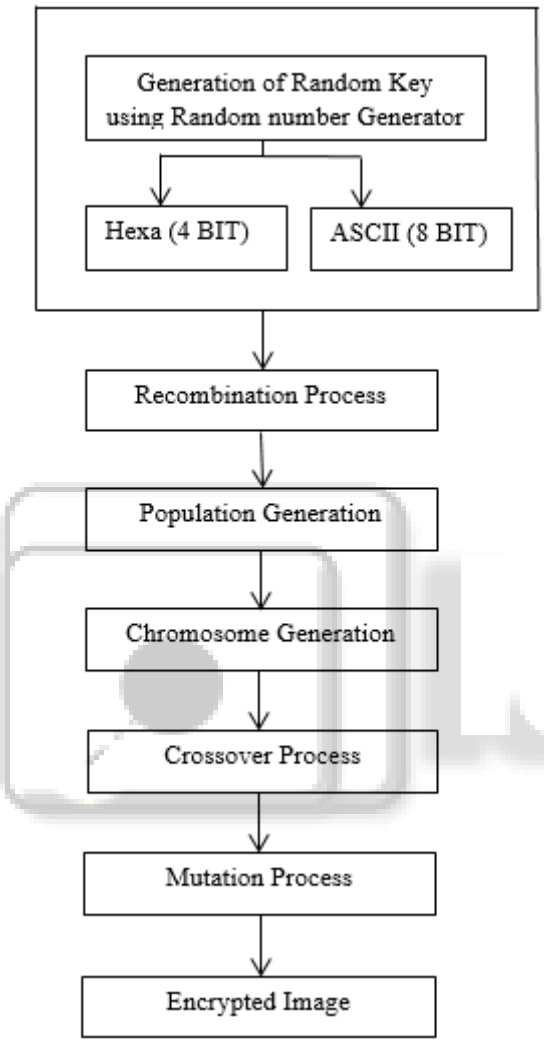

Fig. 3: Flowchart of Proposed Design

VII. RESULT

The Image is transfer after the encryption at the time of communicating or transfer the image, we transfer the encrypted image for the protection of the original image. As shown, fig. 4(a) is the original image and fig. 4(b) is the encrypted image.

The Histogram analysis depicts pixels distribution within an image by representing their number relative to each or every intensity level. We have analyzed the histograms of fig. 4(b) encrypted images as shown in fig. 4(d) and their corresponding plain images fig. 4(a) having widely different contents as shown in fig. 4(c).

Fig. 4: (a)

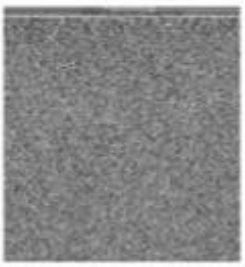

Fig. 4: (b)

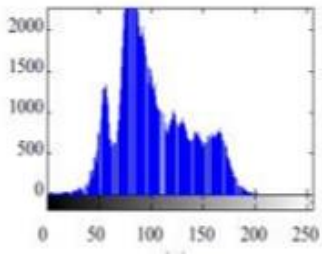

Fig. 4: (c)

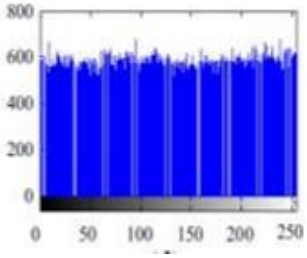

Fig. 4: (d)

REFERENCES

[1] T. L. Takano, Ed., Computed Radiography. Springer-Verlag, 1987, pp. 1–6.
[2] R. C. Gonzalez and R. E. Woods, Digital Image Processing. New York: Addision- Wesley, 1993, p. 27.
[3] M. I. Sezan, A. M. Tekalp, and R. Schaetzing, "Automatic anatomically selective image enhancement in digital chest radiography," IEEE Tran. Med. Imag., vol. 8, pp. 154–162, 1989.
[4] R. H. Sherrier and G. A. Johnson, "Regionally adaptive histogram equalization of the chest," IEEE Trans Med. Imag., vol. MI-6, pp. 1–7, 1987.
[5] M. L. Giger, K. Doi, and H. MacMahon, "Automatic detection on nodules in peripheral radiography," Med. Phys., vol. 15, pp. 158–166, 1988.
[6] A. Nakamori, K. Doi, V. Sabeti, and H. MacMahon, "Automated analysis of sizes of heart and lung in digital chest images," Med. Phys., vol. 17, pp. 342–350, 1990.
[7] E. Pieka, M. F. McNitt-Gray, and H. K. Huang, "Computer-assisted phalangeal analysis in skeletal age assessment," IEEE Trans. Med. Imag., vol. 10,

