ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

*Volume - 5, Issue - 2, March – April - 2019, Page No. 97 - 101*

# Image Encryption Using Genetic Algorithm

Naveen Tiwari, Bhavya Sareen, Anagha Sharma

Assistant Professor, Department of CSE, Arya College of Engineering and Research Centre, Jaipur

**Abstract**

This paper presents a new mathod for image encryption using genetic algorithm. First,rows and columns of the input image are dislocated randomly. Then, the obtained image is divided into four equal sized sub-images.after selecting one of these sub-images accidentally,two pixels are choosen from it as GA intial population.Cross-over and mutation operations are applied on thebinary values of the selected pixels.. These images on the internet will not be secure.Then the image is reconstructed in the reverse manner. Due to the rapid growth of digital communication and multimedia application, security becomes important issue of communication and storage of images. Encryption is one way to ensure high security. Images are used in many areas, such as medicine, military science. Modern cryptography provides information to protect information and protect multimedia data. In recent years, encryption technology has developed rapidly, and several image encryption methods have been used to protect sensitive image data. In this paper, different image encryption techniques have been discussed from which researchers can get an idea for efficient techniques to be used and also discusses the basic image security techniques, the survey of the recent research in the field of image securities like ANN Based Approach, Genetic Algorithm Based Approach, DCT based approach, chaos-based approach, SVD based approach, cryptography based approach.

**Keywords:** Cryptography, Decryption, Encryption, Image Encryption, Genetic Algorithm.

## Introduction

A copy of the communication method used in the different regions, the mediator, the search area, the negotiation area, the military zone, etc. Transferring important photos is taking a trip from an unsafe internet. From this moment on, you must choose a security service so one can imagine that a person cannot access important information. Wind effect for image cubes that need more multimedia data and protection [1]. Cryptography is a systematic image tool. It provides a safe way to transfer and purchase travel photos online. Security is the primary concern of any system to maintain the integrity, confidentiality and validity of the image. At least coding is the optional method, but so is the issue of relative gravity and gray scale data.

Data confidentiality has become unacceptable for data access and the increasing demand for digital signal transmission, data monitoring software has become a critical problem. Various encryption schemes are necessary to protect information from unauthorized access or cloning and illegal modification. Encryption is used in a non-editable format to modify the original data. The great complexity involved in the central generation process makes it difficult for the glass attack to break the key.

Genetic algorithms are new models of adaptive agricultural research algorithms based on natural selection and the mechanism of natural genetics. It belongs to the category of evolutionary algorithms to solve optimization problems that are used according to biological evolution mechanisms, such as mutation, interchange, selection and inheritance (Mitchell

1996, Haupt and Haupt) 2004): the main idea of the random nature of ADC replication for individuals, the population adapts to its environment, the selection process and the behavior of natural systems . This means individual survival and the multiplication of chromosomes that promote the degradation of unwanted properties.

Genetic algorithms [8], 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 uterus to examine the search space. Instead, they use payment values known as search ability. This quality may make the GA-2 h than other local search procedures, such as gradient descent or greedy corrupt methods used for optimization. GA was used for a variety of image processing programs, such as conclusion [6], image segmentation, image compression, away from sensitive medical imaging and extraction function of characteristics [7].

**Image Encryption Methods**

With the growing growth of multimedia applications, security is a major problem in communication and image storage, and encryption is a common technology for maintaining image security. Image encryption techniques attempt to convert the original image into another image that is difficult to understand; to maintain the confidentiality of the image between users, in other words, it is necessary that no one knows the content without the decryption key. The process of encrypting normal text messages in encrypted text messages is called encryption. Decryption. Photo and video encryption contains applications in a variety of fields, including online communications, multimedia systems, medical images, telemedicine and military communications. Color photos are transported and stored in bulk over the Internet and wireless networks, which take advantage of multimedia technologies and rapidly evolving networks. In recent years, many methods of color image encoding and use have been widely proposed, such as GA, AES, RSA or IDEA, most of which are used in text or binary data. It is difficult to use directly in multimedia data and is ineffective for coding color images due to the high correlation between pixels. In the case of multimedia data, it is often redundant, bulky and requires real-time communication.

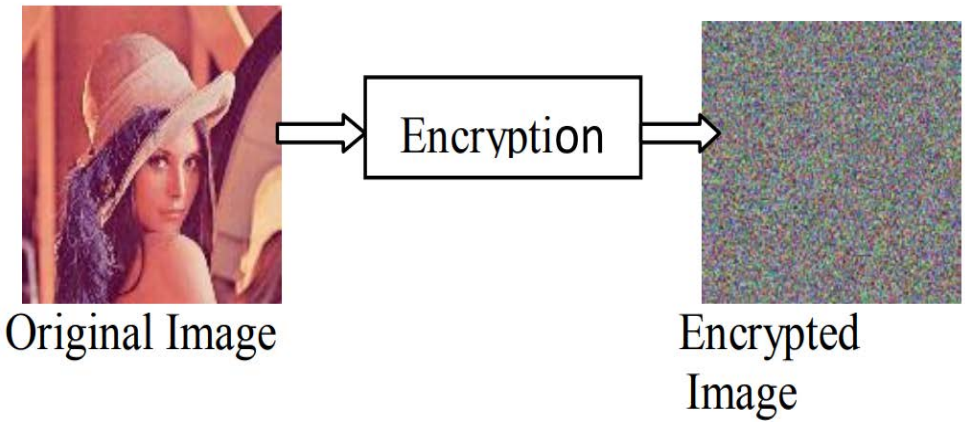


Figure 1 : Image Encryption

**Cryptography**

The many schemes used for enciphering constitute the area of study known as cryptography.

There are three types of cryptography:

**A. Secret Key Cryptography**

This cryptographic method uses one key. The sender uses the key to encrypt the message if the recipient uses the same key to decrypt the message. Because only one key is used, say, this is symmetric encryption. The biggest problem with this method is key distribution, because this algorithm uses one key to encrypt or decrypt.

**B. Public Key Cryptography**

This type of cryptography includes two key cryptographic systems with secure communications. This can occur between the receiver and the transmitter through the communication channel. Since a key pair is used here, this method is also called asymmetric encryption.

This method has a private key and a public key everywhere. Private life is not revealed. The public key is available to all people with whom you want to communicate. When Alice wants to send her a message, Alice is encrypted with Bob's public key, and Bob can decrypt the message with her private key.

**C. Hash cryptography**

This method does not include any keys. Instead, it uses a fixed-length hash value, which is calculated based on a simple text message. Hash functions are used to check the integrity of a message to ensure that the message is not damaged, not damaged, and not affected by viruses. Cryptographic technology requires an algorithm to encrypt data. Currently, when the most important information is stored on computers and transmitted via the Internet, we need to ensure the protection of information. The image is also an important part of our information. Therefore, it is very important to protect our image from unauthorized access.

**Genetic algorithm**

Genetic algorithms simulate biological evolution using the principle of survival of the fittest. Gas has been used in a variety of optimization problems, such as image segmentation, including remote sensing extraction and medicinal properties extraction [7]. Unlike traditional optimization methods, GA uses parallel random search to reach the optimal solution and is less likely to stagnate at the local maximum. In each new generation of the population, it is the birth and fitness values of all individuals that are evaluated in terms of performance in the problem area. The selection, transit and mutation process is repeated until the offspring are produced at an acceptable value.

The General Assembly will randomly study the field of candidate solutions to determine the best (or at least sufficient) solution to a specific problem. A fitness function is used

To rate and compare people based on fitness. The suitability of this selection process is used to identify individuals who can reproduce and spread their genes beneficial to future generations using selection, crossbreeding and mutations.

This process is repeated across successive generations to get a better experimenter or a better solution because of the pros and cons of the problem of incorporating a genetic algorithm for a level segmentation group here. Some of the benefits are as follows on a traditional level.

**A. Flexibility**

The genetic algorithm improves the inherent physical fitness function rather than the explicit one range of power function. This makes them flexible enough to integrate any kind of Characteristic to perform the fragmentation without modifying the fitness function.

**B. Circulation Ability**

Genetic algorithms, like any other evolutionary optimization technique, are usually be more general than traditional optimization methods, since they can be applied to a wide range of features, and may be able to solve different types of segmentation problems combining different types of characteristics. Techniques for strengthen the current laga, to make this circular can be explored in future. Other application areas where delays can be applied in the future are: iris fragmentation of ocular images, hepatic fragmentation in abdominal images and a variety of other image recovery issues that require multiple combinations types of previous information.

**C. Parallel**

SGA evaluates multiple filter solutions in parallel to performance fragmentation. This is quite different from the evolution of the existing menu curve fragmentation techniques that develop only a single partition contour. Parallel it makes the League converge to the global / maximum minimum in the fitness scene.

**Genetic algorithm used in medical image protection**

Genetic algorithms are a powerful adaptation tool for problem solving, research and improvement. It is one of the smart synthesis techniques for improvement. Genetic algorithms are more powerful and better than traditional algorithms. In genetic algorithms, each individual is coded as a vector of variables of limited length and these individuals are bound to chromosomes, then a group of chromosomes forms the population. Genetic algorithms start with a randomly selected group called the first generation, then each individual in the solution-compatible group presents a problem. The fitness function is also known as the destination functions that are formed by combining the two scales which are the noise / peak / peak ratio and link normalization. The fitness function is used to evaluate all individuals in the community and the best individual is evaluated with the corresponding fitness value. The main three companies of genetic algorithms are: Selection, Transit and Mutation Actors applied to chromosomes over and over again. Figure 2 shows the flow chart of the genetic algorithm. Comsawat and Ataktymongkol (2004) developed a technique to optimize the watermark of images using genetic algorithms. It is applied to improve watermark image quality and watermark strength.

**Conclusion**

In this paper, many important encryption techniques have been introduced and analyzed to become familiar with the different encryption algorithms used to encrypt the image that has been transferred to the network. According to the survey of recent research, it has been said that security is the main concern in the transmission of images. The security problem is increasing rapidly with tools developed for hacking image data. Many researchers have proposed solutions to the security problem, but have not been able to obtain complete security on the unsecured network.

**References**


1. G. Miss. Komal R. Hole, Prof. Vijay S. Gulhane, Prof. Nitin D. Shellokar, "Application of Genetic Algorithm for Image Enhancement and Segmentation", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 4, pp-1342-1346, April 2013.
2. Madhu B., Ganga Holi and Srikanta Murthy K, "An Overview of Image Security Techiques", International Journal of Computer Applications, Volume 154 – No.6,pp-37-46, November 2016.
3. Rajinder Kaur and Er. Kanwalpreet Singh, " Comparative Analysis and Implementation of Image Encryption Algorithms", IJCSMC, Vol. 2, Issue. 4, pp- 170 – 176, April 2013.
4. Zhicheng Ni, Yun Qing Shi, Nirwan Ansari and Wei su, "Reversible Data Hinding", IEEE Transactions on Circuits and system for video Technology, Vol-16, No- 3, pp- 354-362, March 2016.
5. Ujjwal Maulik, " Medical Image Segmentation using Genetic Algorithms", IEEE Transactions on Information Technology in biomedicine, Vol-13, No.- 2, pp- 166-173, March 2009.
6. Andrea Valsecchi, Sergio Damas and Jose Santamaria, " An Image Registration Approch Using Genetic Algorithms", IEEE world Congress on Computional Inteligence, pp- 416-419, June 10-15, 2012.
7. Gajendra Singh Chandel, Vinod Sharma and Uday Pratap Singh, "Different Image Encryption Techniques-Survey and Overview", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 8, pp-264-268, August 2016.
8. Shaliza Kaushal, Dr.Vikas Thada and Ms.Aman Jatain, " Effect of Optimization Algorithm on Image Security and Reliability", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5, Issue 5, May 2016.
9. M.Sivagami and P.R.Premkumar,"An Efficient Method Based on Crossover Operation for Image Encryption", IEEE International Conference on Innovations in information, Embedded and Communication System (ICIIECS), pp-1-6, 2017