ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 7, July 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Encryption and Code Breaking of Image Using Genetic Algorithm in MATLAB

Abiban Kumari[1]
M.Tech CSE Scholar
Deptt of CSE, OITM Juglan,
Hisar, India

Shruti Goyal[2]
Assistant Professor
Deptt of CSE, OITM Juglan,
Hisar, India

Abstract: Cryptography is an important technique for protecting information, as the importance of security is increasing day by day. Genetic algorithms are a class of optimization algorithms which is used in this research work. Encryption and decoding of image using genetic algorithm is used to produce a new encryption method by exploitation of the powerful feature of the crossover and mutation operation of genetic algorithm using MATLAB. The proposed algorithm will increase the security and efficiency of the algorithm in term of image security as compare to other algorithm with symmetric key. The proposed methods based on genetic algorithm which is used to generate key by a random number generator. After the examination of the proposed method, it is clear that this method of encryption and code breaking is satisfied the main motive of our research that is required method for image encryption.

Keywords: Cryptography, Encryption, Genetic Algorithm, MATLAB.

I. INTRODUCTION

Computer data travels from one computer to another, leaving the safety of its protected physical surroundings. The protection of data is becoming very important, in the present time. The protection of images data can be done with encryption [7] using different algorithms. There are so many different techniques should be used to protect high level confidential data from unauthorized access. Security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption techniques helps us to convert original image to another image (encrypted) that is not easy to understand; so, to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption [5]. Data security has a major role in the development of communication system, where more randomization in the secret keys increases the security as well as the complexity of the cryptography algorithms. In the recent years network security has become an important concern. Cryptography plays a vital role in the information security system against various attacks. Efficient and newer versions of cryptography techniques can help to reduce this security threat. The Chaotic and Advanced Encryption Standard is a strong symmetric key cryptographic algorithm [6]. The ability to protect and secure information is essential to the growth of electronic commerce and data security. Cryptography is probably the most important technology for protecting data. The digital image becomes very important, especially, in the process of mutual transition of images through open network.

In this study, genetic algorithm is typically used to obtain solution for optimization and search problems. We propose a new approach for e-security applications using the concept of genetic algorithms with pseudorandom sequence to encrypt and decrypt data stream. Many different image encryption methods have been proposed to keep the security of these images. Image encryption algorithms try to convert an image to another image that is hard to understand.

Genetic algorithms (GAs) are search methods based on principles of natural selection and genetics [2]. The GA goes through the following cycle: Evaluate, select, mate, and mutate until some stopping criteria are reached. Reproduction and crossover together give genetic algorithms most of their searching power. The genetic algorithm is a search algorithm based on the mechanics of natural selection and natural genetics [1].

MATLAB is a modern programming language environment used in this study: it has sophisticated data structures, contains built-in editing and debugging tools, and supports object-oriented programming [8]. These factors make MATLAB an excellent tool for teaching and research. MATLAB has many advantages compared to conventional computer languages (e.g., C, FORTRAN) for solving technical problems [4]. It has powerful built-in routines that enable a very wide variety of computations. Application of MATLAB in combination with genetic algorithm is a predominant tool in this work for the programming of image encoding and decoding. On the other hand MATLAB provide us a good graphical representation of the processed images [8].

So, in this work our prime motive is to prevent the theft of or damage to the information using new approach of Genetic Algorithm is proposed in which, the operations of GA (Crossover and Mutation) are exploited to produce new encryption method. Strict procedures for access to the machine room are used by most organizations, and these procedures are often an organization's only obvious computer security measures. Today, however, with pervasive remote terminal access, communications, and networking, physical measures rarely provide meaningful protection for either the information or the service; only the hardware is secure. Nonetheless, most computer facilities continue to protect their physical machine far better than they do their data, even when the value of the data is several times greater than the value of the hardware.

II. RESEARCH METHODOLOGY

Steps of image encryption and Decryption:

- ➢ Loading an image
- ➢ Calculate the Height (H) and Width (W) of image
- ➢ Check the result of H*W mod 8. If equal to 0 then go to 4th step, otherwise doing H = H+(8- (H*W mod 8)) and W = W+(8- (W*H mod 8))
- ➢ Dividing the image into sets of block each block size's (8*8)
- ➢ Select two strings one horizontal and other is vertical.
- ➢ String change into octal .Than we find new string.
- ➢ Doing crossover operation on randomly selected chromosomes.
    - Select randomly two string from the block.
    - Random location from string selected.
    - Swap string together the portion of string on right side.

Let two Strings:

B0	B1	B2	B3	B4	B5	B6	B7

C0	C1	C2	C3	C4	C5	C6	C7

After perform crossover operation:

B0	B1	B2	B3	C4	C5	C6	C7

C0	C1	C2	C3	B4	B5	B6	B7

- Doing mutation operation
- Encryption process is done. Then go to step 2
- Crossover and mutation process done again
- Getting the decryption image
- Mutation and crossover operators repeat for all blocks

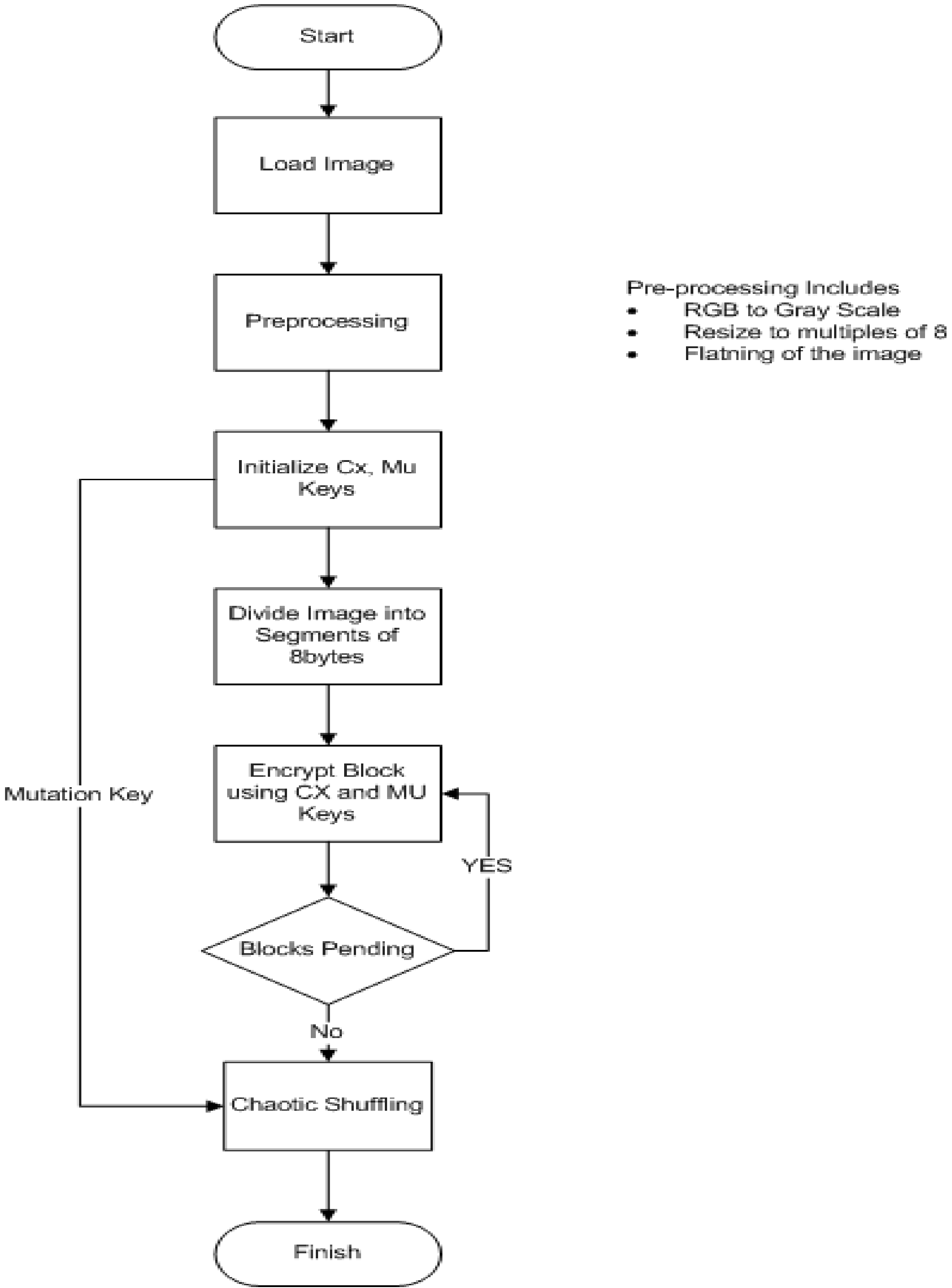


Figure 1: Processing of Encryption and Decryption

III. Results and Discussion

The proposed encryption algorithm can be classified as multiple criteria such as better performance, rapid method of encryption and code breaking of images which is having different shape and size. The test images employed here show positive result. The encryption and decryption algorithm are implemented directly in the MATLAB version 7.10.0.499 (R2010a) 32- bit (win32). The decryption algorithm takes micro seconds to get executed. Similar results were obtained in the study done by Gamil et, al,.[3]. They have proposed an algorithm that will increase the efficiency of the algorithm in terms of computation time required and complexity to attack. To decrypt one block, they have used 16 bit with possible number and to decrypt the whole image as compare to [3], in present study we have used 32 bit with possible number.

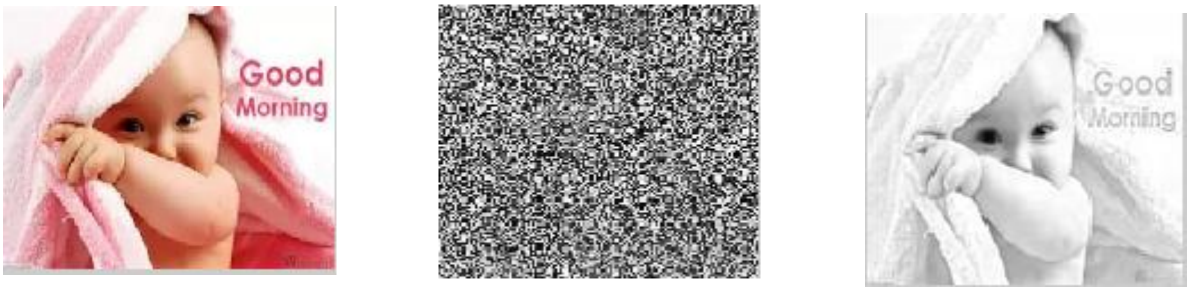
Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. By default, entropy uses two bins for logical arrays and 256 bins for uint8, uint16, or double arrays. If entropy (I) has more than two dimensions, the entropy function treats it as a multidimensional grayscale image and not an RGB image.

When we use RGB channel then the decrypted image will be in the same color as in the original image but it will give us the color image with certain limitations:

- Time complexity will be increase.
- Redundancy will also increase
- Entropy of the image will be only in two dimensions

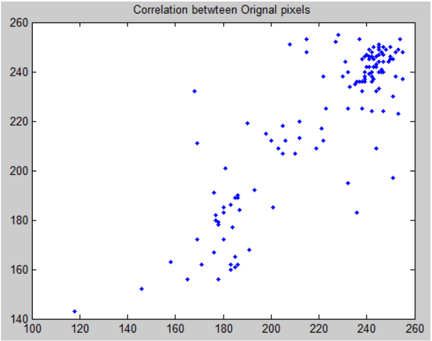
So to overcome such type of limitation, in this research work we have used only single channel (R channel) with entropy has more than two dimensions and with more than two dimensions a single channel will provide us multidimensional grey scale image. Thus, a single channel will give us grayscale image with following advantages:

- Multidimensional image can be encrypted
- Time complexity will be decrease.
- Redundancy will also decrease



Original Image Encrypted Image Decrypted Image

Figure 2: Image(1) at different stages (Original Image, Encrypted Image and Decrypted Image).



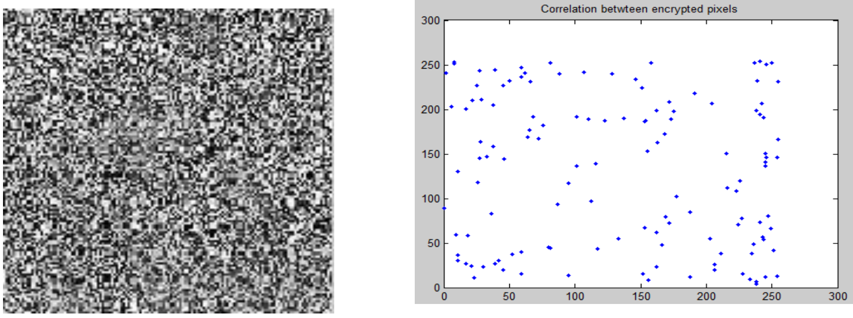
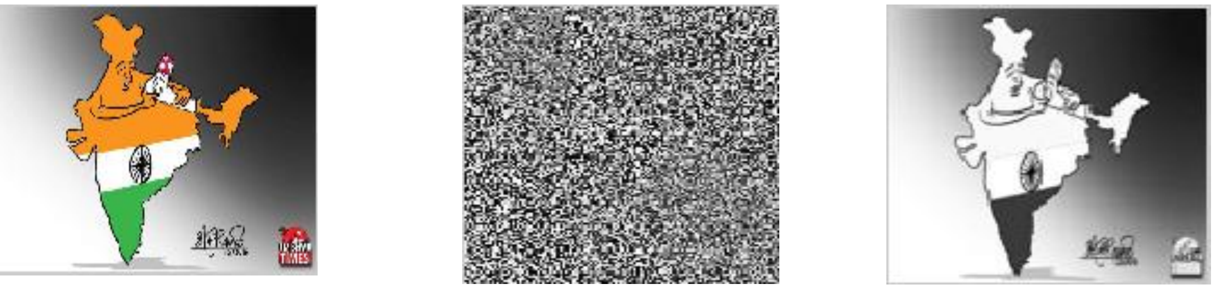


Figure 3: Correlation between Original Image and Encrypted Image



Original Image(2) Encrypted Image Decrypted Image

Figure 4: Image(2) at different stages (Original Image, Encrypted Image and Decrypted Image).

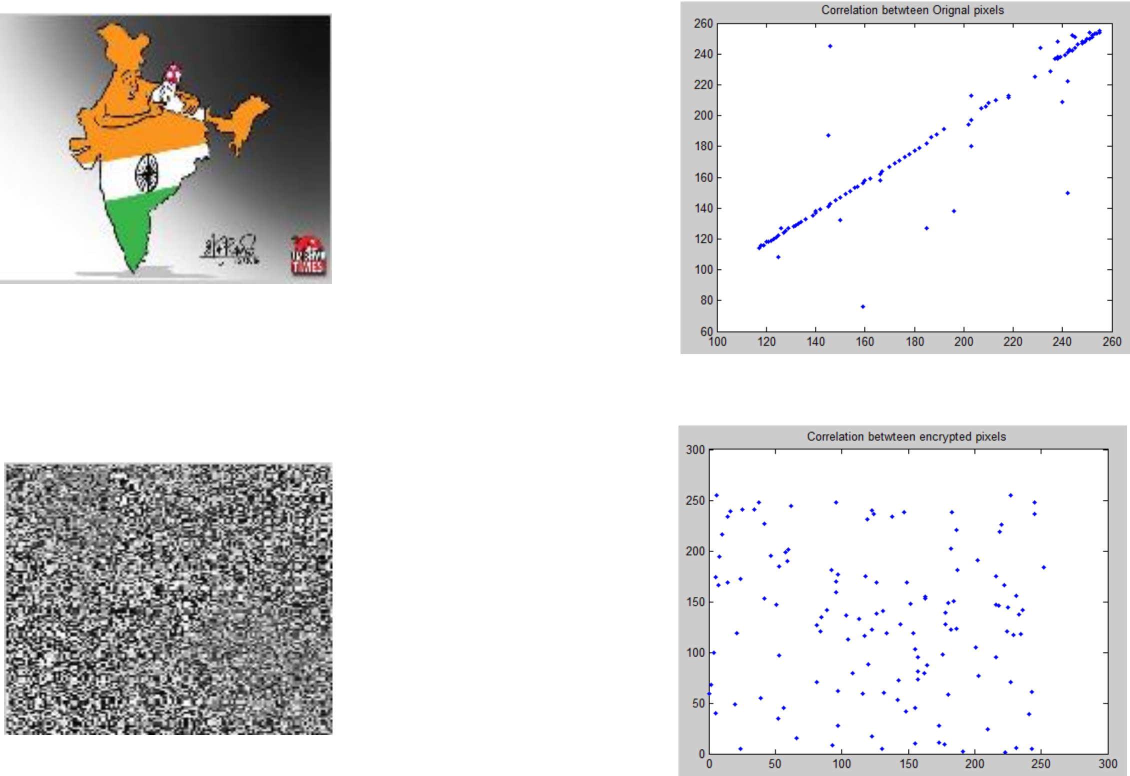


Figure 5: Correlation between Original Image and Encrypted Image(2)

Table 1: Difference between original and final entropy

Entropy (I)		
Sr. No.	**Original Entropy**	**Final Entropy**
1	7.224132	7.986076
2	7.224521	7.970498

It shows that there is no significant difference in the characteristic feature of the original and final entropy of the image.

A statistical analysis which is used in present study has been made by calculating the histograms, the entropy, the correlations and differential analysis for the plain image and the encrypted image to prove the strength of the proposed algorithm for the security of the image data. After testing various images which is having different shape and size, it appears that the intensity values of encryption and decryption are better as compare to the pervious study done so far.

IV. Conclusion

In this research work, a new approach for the image encryption algorithm is proposed. This algorithm shows the relationship between the original and encrypted image based on the genetic algorithm. R channel with symmetric key is used for the encryption of image. The proposed encryption algorithm proved that there is no significant difference in the characteristic feature of both encrypted and decrypted image. So, it is concluded that the when compared to the commonly used algorithm, the proposed algorithm result in the better performance and higher entropy.

References

1. Burke, E. K., Elliman, D. G. and Weare, R.F. Specialised recombinative operators for timetabling problems, in: Evolutionary Computing: AISB Workshop 1995 T. Fogarty, ed., Lecture Notes in Computer Science, Vol. 993, pp. 75–85, 1995, Springer, Berlin.
2. Fraser, A. S. Simulation of genetic systems by automatic digital computers. II: Effects of linkage on rates under selection, Austral. J. Biol. Sci. 10:492–499, 1957.
3. Gamil R. S. Qaid, Sanjay N. Talbar. "Encrypting and Decrypting Images by using Genetic Algorithm": An International journal (ELSEVIER), 2002..
4. The MathWorks Inc. MATLAB 7.0 (R14SP2). The MathWorks Inc., 2005.
5. Sandeep kaur, Sukhpreet Singh, Sonia. A review on Image encryption techniques. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 3, May – June 2013.
6. Rekha Raj, Salim Paul. Image encryption using chaotic maps of various dimensions: Review, International Journal of Research in Engineering and Technology. Volume: 05 Issue: 04 , Apr-2016.
7. Komal D Patel, Sonal Belani. "Image Encryption Using Different Techniques" A New Approach International Journal of Emerging Technology and Advanced Engineering (ijetae) Volume 1(1), 2011.
8. S. J. Chapman, MATLAB Programming for Engineers. Thomson 2004.

Author(s) Profile

Abiban Kumari, received the B.Tech. degree in Information Technology from Guru Jambheshwar University of Science & Technology, Hisar, Haryana. Currently she is pursuing his M. Tech. degrees in Computer Science & Engineering from Department of Computer Science and Engineering, from Om Institute of Technology and Management, Hisar, Haryana, India

Shruti Goyal, received the M.tech degree in Computer Engineering from University Institute of Engineering And Technology, Kurukshetra University, Kurukshetra and B.Tech degree in Computer Science & Engineering from Geeta Institute of Management & Technology, Kanipla, Kurukshetra in 2011 and 2013, respectively. She did her M.tech Dissertation on Network Security. She is now with Om Group of Institutions, Hisar as Assistant Prof. in CSE Department.