ISSN 2347 - 3983
Volume 2, No.11, November 2014
International Journal of Emerging Trends in Engineering Research
Available Online at http://warse.org/pdfs/2014/ijeter032112014.pdf

COMPARISON OF GENETIC ALGORITHM OF IMAGE ENCRYPTION WITH NEW CIPHER ALGORITHM

[1]Rohit Kumar, [2] Shekhar

[1]*M. Tech Scholar, Department of Comp.Sci.and Engg., Graphic Era University, Dehradoon*
[2] *M. Tech Scholars, Department of Comp.Sci.and Engg., RCE, Roorkee*

[1] kambojrohit42@gmail.com
[2] sshekharvnsit@gmail.com

***Abstract*— Network security is an important issue, and encryption is one of the way to ensure security in the digital world. Image security becomes important because of their frequency of use over internet. There exist many different image encryption techniques each has their own advantage and disadvantage. In this proposed method we first encrypt the image using Genetic algorithm and then by using our new cipher algorithm. We have also calculated the PSNR and MSE of reconstructed image of both methods and it is found that our new cipher has higher PSNR and less MSE compared to Genetic algorithm. Thus the image quality of this new cipher is good.**

***Keywords*— Encryption, PSNR, Cryptography, Crossover, Mutation, MSE**

1.INTRODUCTION

The growing dependence [1] on computers to process information and transmit it across virtually connected systems has increased the need for security. Cryptography follows a set of mathematical techniques to provide information security, confidentiality, data integrity, authentication and non- repudiation. There are two types of cryptographic schemes based on the key used:

1.1. Symmetric Cryptography

Here same key is used for encryption and decryption. Symmetric key cryptography is one of the most important types of cryptography where key is shared between both the communicating parties. Symmetric key cryptography is used for private encryption of data to achieve high performance. For e.g. AES, IDEA, DES, etc.

1.2. Asymmetric Key Cryptography

Two different keys are used in Asymmetric cryptography where key for encryption is known as the public key, and the other for decryption, known as the private key. For e.g. RSA, Diffie - Hellman.

The Genetic Algorithm (GA) [3] relies primarily on the creative effects of sexual genetic recombination (Crossover) and the exploitative effects of the Darwinian principle of survival and reproduction of the fitness. Mutation is a second operation in Genetic Algorithm (GA). The crossover operation involves the exchange (swap) between two selected bytes (i.e., string of bits) the crossover points are randomly chosen. For example:

- Consider the data {24, 50, 30, 55, 60, 105}
- Consider crossing over at points 1 and 4 and swap the values at these positions to result {55, 50, 30, 24, 60,105}

The mutation operation is used to randomly alter the value at a single position in the data by applying a function. For example:

- Consider the data {24, 50, 30, 55, 60, 105}
- Consider the mutation operation applied at point 3 by using the function f(y)=255-x to result {24, 50, 225, 55, 60, 105}

***PSNR and MSE*:** Peak signal to noise ratio (PSNR) is most commonly used to measure the quality of reconstruction of encryption codecs (e.g., for image encryption). The signal in this case is the original data, and the noise is the error introduced by encryption. When comparing orignal image and image after encryption and decryption process, PSNR is an *approximation* to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality

PSNR is most easily defined via the Mean square error (*MSE*). Given a noise-free *m*×*n* monochrome image *I* and its noisy approximation *K*, *MSE* is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear PCM with *B* bits per sample, MAX_I is $2^B - 1$.

2.RELATED WORK

Over the years many different methodologies have been introduced for image encryption for secure transmit ion of images over networks .Previous encryption schemes such as, AES DES and T-DES are not well suited to make the cryptosystem for digital images, the main cause of this the inherent features of the images and high redundancy. Some related work is explained below:

A) **Image Security via Genetic Algorithm:** [1] In this paper, a new method based on a hybrid model composed of a genetic algorithm and a chaotic function is proposed for image encryption. In the proposed method, first a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. In each stages of the genetic algorithm, the answer obtained from previous iteration is optimized so that the best encrypted image with the highest entropy and the lowest correlation coefficient among adjacent pixels is produced.

B) **Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique :** Several traditional encryption schemes have been [2] analyzed and based on the literature survey, it has been found that chaotic sequences are very much useful to create randomness. In this paper, a new encryption scheme has been proposed with two phases. In the first phase the input image is transformed using a new transformation technique whereas in the second phase .Chirikov Standard Map is used for pixel shuffling and modified Logistic Map is used for diffusion. Chirikov standard map , decor relate the strong relationship among adjacent pixels hence employed to shuffle the pixel positions of the plain image. The modified logistic map is used for generating the random sequence which is completed the purpose of changing pixel values. Various images and standard lena image is used to demonstrate the validity of the proposed algorithm. The results of experiments show that the proposed algorithm for image cryptosystems provides a no correlation between the original image and cipher image. The scheme is key sensitive and shows impressive resistance against brute force attack and statistical attack.

C) **Bit-Level Encryption of Images using Genetic Algorithm:** It is to be noted that there is a kind of sameness in pixels are changed positions or the blocks are jumbled [3] or the arbitrary bits are added to the pixels in order to encrypt the image. These algorithms might be very effective now, but one day, they might be cracked because of the sameness in the modus operandi of these algorithms. Hence there is a need for a new dimension of thinking in the field of image encryption and hence forth we propose this technique where actually the image encryption is done using breaking and merging of bits. As followed in other encryption techniques the image is first broken down into blocks also known asa grid. Then the initial transformation steps are performed and then 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.

D) **A new approach for data encryption using genetic algorithms:** In [4] e-applications security, integrity, non-repudiation, confidentiality, and authentication services are the most important factors. This paper deals with the confidentiality of electronic data which is transmitted over the internet. We propose a new approach for e-security applications using the concept of genetic algorithms with pseudo random 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.

E) **Bit-Level Encryption and Decryption of Images Using Genetic Algorithm:** A New Approach : Encryption is one of the [5] popular methods to achieve secret communication between sender and receiver. In current time the security of digital images draws more attention, especially when these digital images are stored in memory or send through the communication networks. Many different image encryption techniques have been proposed to save the security of images. Image encryption techniques try to convert an image to another image that is hard to understand. Genetic Algorithm (GA) has been popular in the encryption image because of its intuitiveness and ease of implementation. This paper proposes a method based on Genetic Algorithm (GA) which is used to produce a new encryption method by exploiting the powerful features of the Crossover and Mutation operations of (GA). It is a new approach of genetic algorithm (GA) with pseudorandom sequence to encrypt image stream. The feature of this approach includes high security and high feasibility for easy integration with digital image transmission applications. The experimental results of the proposed technique confirmed that high throughput rate required for real time data protection was achieved.

F) **Using Genetic Algorithm for Symmetric key Generation in Image Encryption:** Cryptography is essential for protecting information as the importance of security is increasing day by day with the advent of online transaction processing and e commerce. In now a day the security of digital images attracts much attention, especially when these digital images are stored in memory or send through the communication networks. Genetic algorithms are a class of optimization algorithms. Many problems can be solved using genetic algorithms through modeling a simplified version of genetic processes. In this paper, I proposed a method based on Genetic Algorithm which is used to generate 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 we can keep the strength of the key to be good, still 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.

3.IMAGE ENCRYPTION USING GENETIC ALGORITHM

The encryption method using Genetic algorithm consists of the following [1] steps:

Step (1): Consider an image I(WxH), such that W and H are the width and height of T. Split the image I to a set of N vectors of length L (L = 64 bytes in this work).

Step (2): Then find R1 and R2 from the equations:

$$R1 = \sum_{i=0}^{W-1} \sum_{j=0}^{H-1} (-1)^{(i+j)} * I(i,j)/256*L$$

$$R2 = \sum_{i=0}^{W-1} \sum_{j=0}^{H-1} (-1)^{(i+j+1)} * I(i,j)/256*L$$

Assume the value (R1+R2)/2 as the start value of any known random number generation algorithm used that is used in this encryption method.

Step (3): Set x=R1 and y=R2.

For I = 0... N-1 set the following information for each vector Vi from the set of N vectors:

- Crossover index = x
- Crossover iteration = V1(x)
- Mutation index = y
- Mutatiori iteration = Vjy

x = x+1 y=y+1

If (x or y) > **L** then set x = 0 and y =0.

Step (4): For i = 0... N-1, perform *Step (5)* and Step (6) for each vector Vi from the set of N vectors. Note that both values in Vi (Crossover index) and Vi (Mutation index) are not participate in the crossover and mutation operation.

Step (5): (crossover operation)

- Set Crossover index of vector Vi as a new start value of the adopted random number generation algorithm.

- For j from 0 to Crossover iteration of vector Vi, generate two random numbers N1 and N2 with values between (0..L-1), then perform Vi(N1)⟷Vi(N2).

Step (6): (mutation operation)

- Set Mutation index of vector Vi as a new start value of the adopted random number generation algorithm.
- For j from 0 to Mutation iteration of vector
  Vi, generate one random number N1 with values between (O..L-1), then perform Vi(N1)= *255-Vi(N1).*

Step (7): Construct an encrypted image from the set of N encrypted vectors that are produced from the Step (4). Then hide the values R1 and R2 in the encrypted image.

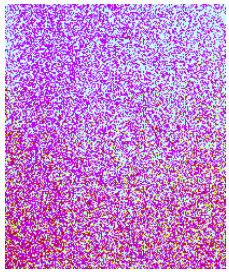
Certainly, the proposed decryption method is done in the reverse form of the above encryption method.

4. ENCRYPTION USING NEW CIPHER

The new algorithm makes use of a new cipher and genetic algo to encrypt the image. The algorithm makes use of a cipher matrix, in which we first take a zero matrix then we generate some random numbers and XOR with zero matrix to form cipher matrix. After this we replace the original image matrix values by cipher matrix using a function. In the resultant matrix crossover operation of genetic algo is performed to form encrypted image. It consist of following steps.

```
/* Setup */

Step1. I  ← read image file
Step2. Get size of image r and c  (rows and columns)
Step3. x ← call function to get ciphered matrix
Step4. x  ←uint8(x)  // convert double to unsigned
integer 8
Step5. x ←128.*x      // multiply cipher matrix by 128
Step6. sort x matrix
Step7. v1 ←x          //initialize v1 to store encrypted
image at stage I

/* Encrypt */

Step8. for k  1  to d     //dimension
Step9.  for i   1   to r
Step10.for j    1 to   c
Step11. v1(i,j,k) ←  (x(i,j,k) - xx(i,j,k))/2     //xx is
original image
Step12. end for
Step13.end for
Step14.end for

/* sort encrypted image  */

Step15.  v2 ←sort(v1)

/*    interchange positions   */

Step16. for k ←1  to d
Step17. for i←1 to r
Step18. for j=1: c-1
Step19. Temp ←v2(i,j,k);
Step20. v2(i,j,k) ←v2(i,j+1,k);
 Step21.v2 (i,j+1,k)=temp;
Step22. end for
Step23. end for
Step24. end for

% multiply each element of the image by 128
Step25.  for k ←1   to d
Step26.  for i ←1 to r
Step27.   for j ←1 to c
Step28.   v2(i,j,k) = v2(i,j,k)*128;
Step29.   end for
Step30.  end for
Step31.  end for


/*  decrypt  */
Reverse the above steps to de-cipher the image

/*  Cipher function

Step1. Initialize required variables
Step2. t ←zeros(r,c,k)   // generate zero matrix
Step3. for k  ←1 to 3
Step4. for i <-1  to r
Step5. for j ←1 to c
Step6. x(i,j,k)  ← randi(i) //store random number
Step7. end for
Step8. end for
Step9. end for
Step20.x ← bitxor(x,t);
Step21.end function
```

6.EXPERIMENTAL RESULTS



a) Input image **b) Encrypted image**

Fig: Image encryption using genetic algorithm

a) Input image **b) encrypted image**

Fig: Image encryption using proposed algorithm

Comparison: We have calculated mean square error and peak signal to noise ratio of several images using both the algorithm. And it is clear that our proposed algorithm has less mean square error and large peak signal to noise ratio. Thus the quality of image after decryption in proposed algorithm is good compared to that of in genetic algorithm.

Name of image	MSE of Genetic algorithm	MSE of New algorithm	PSNR of Genetic algorithm	PSNR of New algorithm
Water lilies.jpeg	0.237412	0.0293427	54.5533	72.2451
Winter.jpeg	0.291234	0.0229837	58.4491	98.9756
Sunset.jpeg	0.783492	0.0189378	109.9823	158.9876

Table1

7.CONCLUSION

After the experiments of the proposed encryption method, it is clear that this encryption method satisfied the goals that are required in any encryption method for encrypting the image. The new encryption method has large PSNR and less MSE compared to genetic encryption method used, thus the quality of the image after decryption in new method is good.

References

[1] Rasul Enayatifar and Abdul Hanan Abdullah, "Image Security via Genetic Algorithm", *2011 International Conference on Computer and Software Modeling IPCSIT vol.14 (2011) © (2011) IACSIT Press, Singapore*

[2] Nidhi Sethi and Sandip Vijay, "Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique", Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013)

[3] V.Srikanth1, Udit Asati, Viswajit Natarajan, T.Pavan Kumar, Teja Mullapudi and N.Ch.S.N.Iyengar, "Bit-Level Encryption of Images using GeneticAlgorithm", TECHNIA International Journal of Computing Science and Communication Technologies, VOL. 3, NO. 1, July 2010 (ISSN 0974-3375).

[4]Abdel salam, Aalmarimi, Anil Kumar, Ibrahim Almerhag and Nasreddin Elzoghbi, "A NEW APPROACH FOR DATA ENCRYPTION USING GENETIC ALGORITHMS" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 9, 2012.

[5] Gamil R. S. Qaid and Sanjay N. Talbar, "Bit-Level Encryption and Decryption of Images Using Genetic Algorithm: A New Approach" *IPASJ International Journal of Information Technology (IIJIT)* Volume 1, Issue 6, December 2013 ISSN 2321-5976.

[6] Aarti Soni and Suyash Agrawal, "Using Genetic Algorithm for Symmetric key Generation in Image Encryption", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012.

[7] Issa A. Abed ´, "Finding the Best Key Stream by Using Genetic Algorithm for Image Encryption", Journal of Basrah Researches ((Sciences))Vol. 36, No. 3, 15 June ((2010)).

[8] Sindhuja K , Pramela Devi S, "A Symmetric Key Encryption Technique Using Genetic Algorithm", Sindhuja K et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 414-416.

[9] Shubhangini P.Nichat*, Prof.Mrs.S.S.Sikchi, "Image Encryption using Hybrid Genetic Algorithm International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 1, January 2013 ISSN: 2277 128X.

[10] Aarti Soni, Suyash Agrawal, "Key Generation Using Genetic Algorithm for Image Encryption," International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 2, Issue. 6, June 2013.