IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-5 E-ISSN: 2347-2693

A Parallel AES of Faster Image Transfer Using Genetic Algorithm Key Generation

Suvarna Patil1* and A.D Thakare[2]

[1*,2]Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering,
Savitribai Phule, Pune University, India

www.ijcseonline.org

Received: May/02/2015 Revised: May/10//2015 Accepted: May/24/2015 Published: May/30/ 2015

***Abstract*—** Now exponentially increased the use of information exchange and the multimedia applications. Security is the essential criterion in cryptography for the transmission of data or message in the secured form in all the applications. For preserving the privacy of data onto different applications encryption is a crucial technique. Advanced Encryption Standard algorithm is used for encrypting the image. The genetic algorithm is an important method of solving the optimization problem. This paper is based on the genetic algorithm used for making the encryption key stronger. Using parallel AES algorithm the experimental results show that it improves the fastness of the AES algorithm and meet the security demand.

***Keywords*—** AES, Genetic Algorithm, Cryptography, HD Image, Security

I. INTRODUCTION

There is large amount of data is transferred on the internet; because it is confidential data it requires high security. Cryptography is the technique for the transmission of data or message in the secured form so only authorized person can read the data or message. It is used for providing the security to the data onto the image, audio and video data. For this there are different cryptographic algorithms proposed. Some of the cryptographic algorithms are AES, DES, IDEA, or RSA. For cryptography there are two types of text formats is used one is plain text that sends from sender to a receiver and another is cipher text that is the encrypted message. There are two different types of cryptography:

A. Public key cryptography
B. Private key cryptography

The Public key cryptography is also called as asymmetric key cryptography because the sender and receiver using different key, private key for encrypting and public key for decrypting the message. The private key cryptography is also called as symmetric key cryptography because the sender and receiver both using same key called public key to encrypting and decrypting the message.

A. The background of basic AES Algorithm:

The NIST has selected the AES algorithm as a block ciphering algorithm. AES is a strong encryption algorithm which is also called as the ciphering algorithm. On the basis of key there are three types of AES algorithm. One is AES128 bit in which 128 bit block of data is used. Like this AES192 bit and AES256 bit is used. Here used symmetric key to encrypt the sensitive data. The block size is 16, 24 and 32 bytes. The 16 bytes block size is selected by the NIST. For AES the DES is the basic algorithm. The triple DES and double DES are the types of DES algorithm. It breaks easily. The DES is working slowly because of its small block size so it is replaced by a new AES algorithm of variable block size. The AES block cipher is the iterated cipher because several times it repeats the steps. The majority of the encryption algorithms are a reversible type of algorithm. It is easy to implement because it works on fixed number of bytes. The AES algorithm uses secret key or private key for the encryption of data. Both encryption and decryption performed reversely on the AES algorithm.

Corresponding Author: *SUVARNA PATIL, karankal.suvarna@gmail.com*
Department of Computer Engineering, University of Pune, India

B. Requirement for AES algorithm:

The AES algorithm is supporting the three key sizes of N number of rounds, like for 128 bit uses 10 rounds, for 192 bit uses 12 rounds and for 256 bit it uses 14 rounds. Generally it uses 128 bits of block size.
The AES algorithm has to go through the drawback of slow processing for image, video or audio data. It has created patterns of image data. But it has several applications of web browser server, multimedia, cell phone, and medical image. A random number generator is type of device for generating the numbers sequentially. That numbers are appeared randomly.

C. Genetic Algorithm:

The genetic algorithm is actually based on the Darwin's evolution theory. It is called as the heuristic search algorithm. It uses the idea of natural selection and inherent.

In which best offspring is selected for future evolution. The algorithm is based on the concept of survival of the fittest. The genetic algorithm is intended for reproduction in evolution of natural system. It provides an alternative method of finding the optimal result.
In this algorithm each chromosome has one binary string. And characteristics of the individual is shown using to bit of string
The chromosome then looks like this:

Chromosome 1 1101100100110110
Chromosome 2 1101111000011110

In genetic algorithm following are the operations performed like this:

1. Initialization
2. Selection
3. Crossover
4. Mutation

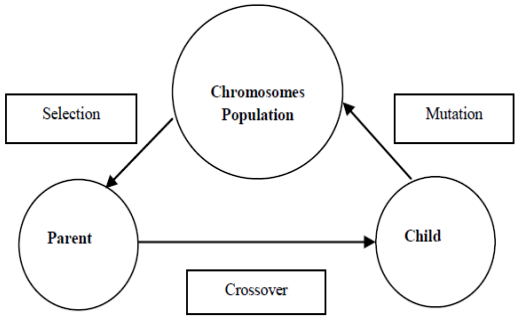


Fig. 1 Model for Genetic algorithm cycle

Initialization: From the population first we selected the individuals. These individuals are represented using the binary string of data.
Selection: In this new population is selected using the existing. A fitness function is used for this.
Crossover: Then from these individuals we have produced new individuals using crossover. In this process it selects some characters of parent chromosomes then it forms new individual. From two parents it selects both the parents' some of the characters.
Example of crossover

Parent 1 1101100100110111
Parent 2 1101111000011111
Child 1 1101111000011111
Child 2 1101100100110111

Mutation: In this process it randomly exchanges one or more bits and gives the best result

II. LITERATURE SURVEY

In this paper [12] for the generation of asymmetric key in encryption and decryption of messages the randomness of crossover and mutation operations are used. The private key is generated using random byte and permutation factor. The permission of sender and the receiver the asymmetric key of permutation factor is defined previously. The number of points is used in crossover and mutation together. Like for crossover, mutation and random byte the points are four, three and single respectively and as well as factor of permutation is considered, so the algorithm strength is increased. The three parameter ranges are in 0 to 15 and last parameter is in the 1 to 7 range. Each parameter is used 4 bits for the consistency. Hence 36 bits key length is considered for this. The permutation and randomness both makes the algorithm strong. This algorithm is more strengthened and hard to break, so the concept may use for any of the file in data transmission purpose.

In this paper [13] a genetic algorithm is used for the communication network design for secure, robust and faster process of cryptography in encryption and decryption. For simplification use single point crossover and block cipher. The Genetic algorithm makes it exceptional. In this work the effectiveness of key is enhanced by key transformation process. It is more secured and not easy idea to break through the attack. In the proposed system the generation of key and some steps are motivated by the DES algorithm.
In this paper [14] the new concept of image encoding using genetic algorithm is introduced. The genetic algorithm is used in secret key encryption algorithm to resolve the problem. Here on component vectors of a picture apply a few rounds often using the crossover and mutation operators. Here on vectors of 8 pixels the several crossover and mutation functions are applied. But for each vector only a single crossover and mutation function is applied. The drawback of this is it can't create the high confused and diffused cipher image. Generally the image may recognize easily from cipher image but in this the cipher image is different completely from the original image and not revealed easily. For attacker requires n number of attack for this cipher image. The results show that it will give the high security and randomness in rounds of crossover and mutation.

Using this paper [15] we can create 10 different keys using new architecture with new proposed algorithm for solving AES key encryption algorithm so the process of expansion and creation is simplified. The concept is dependent on the linear feedback shift register algorithm and genetic algorithm. A schedule key and ciphering key is produced using the genetic algorithm. The schedule key and ciphering key can be expanded by using the modified genetic algorithm. In this the results show that the proposed model is efficient and highly secured. Using the method the AES algorithm complexity is reduced up to fifty percent.

In this paper [16] using the genetic algorithm in public key cryptography the key is selected on the basis of fitness. We

can keep very good strength with the help of genetic algorithm. In this for result analysis different test samples are tested like frequency test, gap test. For random numbers the common tests on the sample are applied. Almost all the samples are apparently satisfy. No repetition was found when analyzing about a five hundred values. The autocorrelation coefficient was calculated and found the better result for random sample with varying length sequences.

In this paper [17] the proposed method of encryption has two phases one is the modification phase and another is the diffusion phase. In phase modification, to reduce the correlation between the neighboring pixels the location of pixels is changed. After doing this in the diffusion phase values of pixels are altered for encrypting the image. For these phases the genetic algorithm binary chromosomes are used. The Local Binary Pattern (LBP) operator is used in modification phase for the generation of binary pattern and the Bit Plane Slicing (BPS) is used in diffusion phase for obtaining the binary chromosomes. In genetic algorithm the initial population has the rows and columns for the input image. A random generator for utilization of predefine the key is used instead of selection of parents from the primary population. In this it is essential to recreate the initial input image for decrypt the image. In both phases of modification and diffusion fitness function is used for average transition in histogram uniformity and LBP image from 0 to 1. By using correlation coefficients, histogram analysis and entropy the encrypted image randomness is measured. Here it shows that the image encryption process can make fast and effective by using the proposed method. In this approach the keys are very sensitive, that means if the small change in that will not at all recover the original image.
This paper [18] uses a new approach of pseudo random generator in data security. In this uses the genetic algorithm for the generation of key by new approach. On current time basis of the system the random numbers are generated. The key strength is maintained by increasing the key irregularity in genetic algorithm. Still a complete algorithm is working properly. If the PRNG is used with genetic algorithm then a complex key is generated in which it is hard for the attacker to attack. In this the symmetric key AES algorithm is used as an efficient algorithm for encryption of image. In general the algorithm efficiency is increased with less computational time.

For providing the security to the image there are many image encryption techniques are developed. In technique of image encryption one image is converted into the other image which is not easy to understand. The genetic algorithm solved the different problems using genetic algorithm simplified version. In this paper [19] a new method is proposed which is dependent on the genetic algorithm to create a method of image encryption of secret key with utilization of useful feature of genetic algorithms crossover and mutation function.

III. WORKING METHODOLOGY

The AES algorithm has the length of 128 bits, 192 bits and 256 bits data and it has a variable block size of 16, 24, 32 bytes. Generally it works on the block size of 16 bytes that constructed in 4×4 matrices which are also called as a state. AES algorithm is working in four different operations: If it performs the encryption operation then the steps are: Add Round Key, Byte Sub, Shift Row and Mix Column. It works recursively if performing the decryption operation and missing the Mix Column step in this process.

In AES algorithm the image ciphering has the problem of similar color pattern appearance present in the original images. Removing this pattern appearance problem of the image I have used the AES algorithm proposed to [9]. Using parallel processing our paper [20] focuses on reducing the encryption and decryption times. Here I implemented the Advanced Encryption Standard algorithm in parallel and genetic algorithm for key generation. In this I analyze the result from different images. Then the experimental results show that the computational time is reduced using a parallel processing. Following is flow chart of given proposed model:

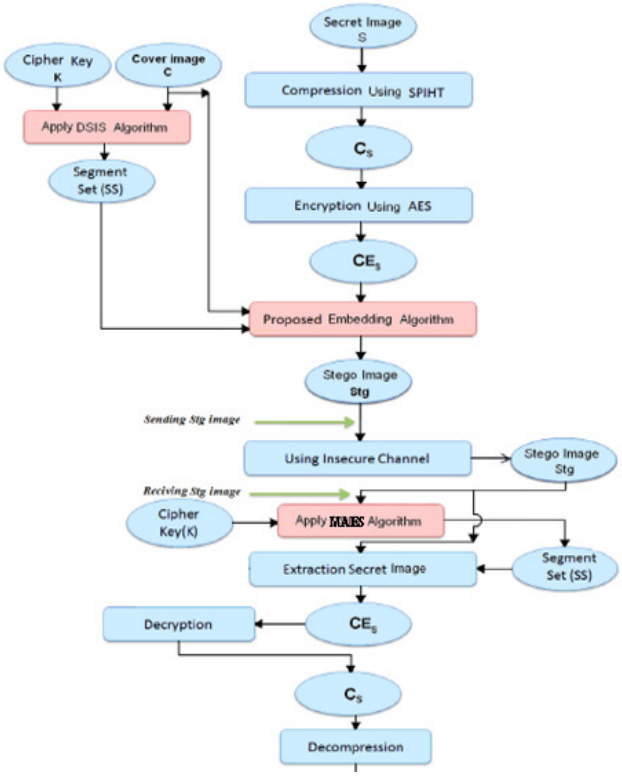


Fig. 2 Flow chart of proposed model

IV. EXPERIMENTAL RESULT

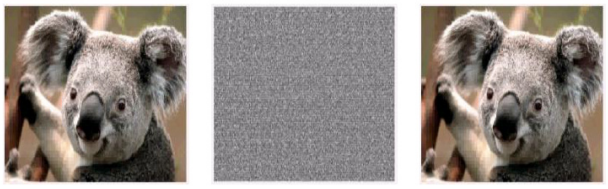
Here in this work first selects initial population. Then the individual is selected on the basis of maximum value of fitness. From this two best individual are selected and apply a crossover function. From this got a child of the individual then all over again apply the fitness function, and find the better child. Later than apply mutation operation on this and get the final key to encryption. Following is the fitness function used in this [11]:

$$F = n + (€/m) \quad (1)$$

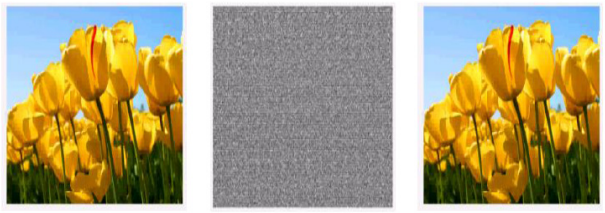
Where, F = Fitness function
n = Sum number of symbols
m = Maximum appeared symbol percentage
€ = Each ideal symbol percentage

Implementation in Dot Net: The proposed method is implemented in the C# dot net 2010 and the analysis is done in the Excel.

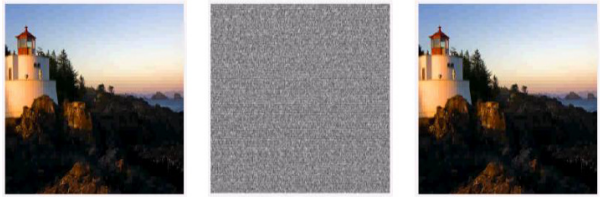
Comparison of Execution Time: Here the time required for the execution of proposed method is very less as compared to the original AES algorithm and a complex key is formed using genetic algorithms. It reduced the time of original algorithms is up to 80% which is the best result achieved using the parallel AES. In this the AES algorithm is carried out on images of the encryption and decryption. At this time I have given just three images of encryption and decryption process from 200 images.



(a) Original Encrypted Image (b) Ciphered Image (c) Decrypted Image



(a) Original Encrypted Image (b) Ciphered Image (c) Decrypted Image



(a) Original Encrypted Image (b) Ciphered Image (c) Decrypted Image

Fig. 3 Modified Algorithms obtained result of application

V. CONCLUSION

Security is the essential criterion of cryptography for the transmission of data or message in the secured form in all the applications. For preserving the privacy of data onto different applications encryption is a crucial technique. Genetic algorithm is an important method of solving the optimization problem. The genetic algorithm is used here for making the encryption key stronger. The key is created using the fitness function The Advanced Encryption Standard suffered from the drawback of more computational time and hardware requirement. The experiment is carried out on more than two hundred samples. Every population is varying from each other. For this 128 bit key is selected. Using our parallel AES the experimental results show that the planned method improves the fastness of the AES algorithm up to 80% and meet the security demand and useful to provide the security in different applications.

REFERENCES

[1] Bhavin Patel, Neha Pandya, "Data Transfer Security Solution for Wireless Sensor Network", International Journal of Computer Application Technology and Research Volume-**2**, Issue **01**, **63-66**, **213**.

[2] Divyani UdayKumar Singh et al, "Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation", International Journal of Computer Science and Information Technologies, Volume **5(3)**, **214**.

[3] Sourabh Singh, Anurag Jain, "An Enhanced Text to Image Encryption Technique using RGB Substitution and AES", International Journal of Engineering Trends and Technology (IJETT) – Volume **04**, **213**.

[4] Salim M. Wadi, Nasharuddin Zainal, "Rapid Encryption Method Based on AES Algorithm for Grey Scale HD Image Encryption", International Conference on Electrical Engineering and Informatics (ICEEI), **213**.

[5] K. Brindha, G. Ramya, Rajpal Amit Jayantila, "Secured Data Transfer in Wireless Networks Using Hybrid Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering , Volume **03**, **213**.

[6] Adam Berent, "Advanced Encryption Standard by Example".

[7] Kamali S. H., Shakerian R., Hedayati M., Rahmani M., "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", International Conference on Electronics and Information Engineering, **210**.

[8] NIST, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, **202**.

[9] Ahmed Bashir Abugharsa, Abd Samad Bin Basari, Hasan Hamida Almangush, "A New Image Encryption Approach using The Integration of A Shifting Technique and The Aes Algorithm", International Journal of Computer Applications (0975-8887), Volume **42**- No.**09**, March **212**.

[10] M. I .Youssef, A. E. Emam, S. M. Saafan, M. Abd Elghany, "Secured Image Encryption Scheme Using both Residue Number System and DNA Sequence", International Journal

of Emerging Science and Engineering (IJESE) ISSN: **2319-6378**,Volume **01**, Issue**12**, October **213**.

[11] Aarti Soni, Suyash Agrawal, "Key Generation Using Genetic Algorithm for Image Encryption", International Journal of Computer Science and Mobile Computing (IJCSMC,), Volume **02**, Issue. **06**, June **213**.

[12] Dr. Poornima G. Naik, Girish R. Naik, "Asymmetric Key Encryption using Genetic Algorithm", International Journal of Latest Trends in Engineering and Technology (IJLTET), ISSN: **2278-621X**, Volume **03**, Issue **03**, January **214**.

[13] Somalina Chowdhury, Sisir Kumar Das, Annapurna Das, "Application of Genetic Algorithm in Communication Network Security", International Journal of Innovative Research in Computer and Communication Engineering, Volume **03**, Issue **01**, January **215**.

[14] Vijaya Madhavi Lakshmi. Challa, Manasa. Bezawada, Anusha. Tenali, "An Image encryption Approach using Multilayer Crossover and Mutation Procedures", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: **2277 128X**, Volume **05**, Issue **02**, February **215**.

[15] Sliman Arrag, Abdellatif Hamdoun, Abderrahim Tragha and Salah eddine Khamlich, "Replace AES Key Expansion Algorithm By Modified Genetic Algorithm", Applied Mathematical Sciences, no. **144**, **7161 – 7171**, Volume **07**, **213**.

[16] Sonia Goyat, "Genetic Key Generation for Public Key Cryptography", International Journal of Soft Computing and Engineering (IJSCE), ISSN: **2231-2307**, Volume **02**, Issue **03**, July **212**.

[17] Roza Afarin, Saeed Mozaffari, "Gray Level Image Encryption", International Journal of Computer, Control, Quantum and Information Engineering, Volume **08**, No:**06**, **214**.

[18] Aarti Soni, Suyash Agrawal, "Using Genetic Algorithm for Symmetric key Generation in Image Encryption", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: **2278 – 1323**, Volume **01**, Issue **10**, December **212**.

[19] Ankita Agarwal, "Secret Key Encryption Algorithm Using Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: **2277 128X,** Volume **02**, Issue **04**, April **212**.

[20] Suvarna Patil, Rahul Patil, "Faster Transfer of AES Encrypted Data over Network", International Journal of Computer Science and Information Technologies (IJCSIT), **7674-7676,** Volume **5(6), 2014**.

[21] R. Kanimozhi, "A Novel Secure Multimedia message Hiding Algorithm behind the Image" SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE), ISSN-**2348-8387**, Volume **01,** Issue **08,** October **214.**

