ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Optimization of Steganography Technique using AES

Sayiema Amin [1], Durfi Ashraf [2], Amardeep Singh Virk[3]

P.G. student, Department of Electronics & Communication Engineering, Adesh Institue of Engineering & Technology, India[1,2]

Associate Professor, Department of Electronics & Communication Engineering,Adesh Institue of Engineering & Technology, India[3]

ABSTRACT: Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Cryptography and steganography can be utilized for securing the information. The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are needed to protect against unauthorized access and use. The two main problems that arise in image encryption are with respect to its time it takes for its computation and its security level. In this paper, a technique is proposed using optimized AES and GA which helps in the security of an image. Strong steganographic technique is proposed which helps to achieve high security. The results obtained are compared with the previous techniques.

KEYWORDS: Image encryption, Steganography, AES, GA, Cryptography

I. INTRODUCTION

With the expanding utilization of the Internet and other effective technologies of communication, the digital media have turned into the most well-known tools which are used to transfer data. A large portion of these digital media are in the form of image and also utilized as a part of different applications, for example, chats, news, websites, e-commerce, email and e books etc. But still digital content is still faced with many difficulties, for example, authentication, tampering and protection of copyright. The modern techniques of encryption have been viewed as the most capable answer for the vast majority of these issues. Tamper detection and content authentication of digital image, audio and video have caught enthusiasm of researchers. Recently, tamper detection, protection, copyright of images and content authentication attracted attention of researchers. In the last ten years, researches on the schemes of security of images concentrated essentially on the issues of protection of copyright, yet gave less consideration on the lossless data, speed and distortion. [1]

The security standard accepts an unmistakable separation between attackers and users and security of network is achieving an attention as the information being shared on the internet increases. Hence, the privacy and security are needed to defend against unauthorized access. This has brought about an explosive growth of the field of hiding of information, which covers applications, for example, Steganography, digital media, fingerprinting, digital watermarking and cryptography. All these applications for hiding of information are truly diverse. Steganography and cryptography are generally used in the field of hiding of data and has gotten consideration from both academia and industry in the past. Steganography gives security and secrecy at very high level by consolidating with cryptography. Until quite later times, the art of cryptography was used regularly and generally by government and area of defense so as to secure privacy of grouped communication. [2]

Cryptography and Steganography are two essential branches of information security. Cryptography gives techniques of encryption for communication to be secure. Cryptography is the technique that studies the techniques of mathematics

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710
International Journal of Innovative Research in Science, Engineering and Technology
(An ISO 3297: 2007 Certified Organization)
Vol. 4, Issue 8, August 2015

for keeping secure messages and also free from attacks. Steganography is the science and art of concealing communication. Steganography includes concealing information so that it creates an impression that no data is covered up by any means. Cryptography and Steganography attain the same objective through distinctive means. Encryption encrypts the information so that an involuntary recipient cannot focus its proposed significance. Steganography, on the contrary endeavors to keep involuntary recipient from expecting that information is there. Combining steganography and encryption considers a superior private communication. The objective of steganography is to abstain from attracting suspicion to the transmission of undisclosed message. Steganalysis is a method for recognizing conceivable secret communication utilizing against steganography. That is, steganalysis endeavors to defeat techniques of steganography. It depends on the way that concealing information in digital media modifies the carriers and presents irregular marks or some type of degradation that could be misused. Hence, it is critical that a steganography system to find out that hidden message is not discernible. [3]

II. ADVANCED ENCRYPTION STANDARD (aes)

Advanced Encryption Standard is the Rijndael algorithm by two researchers Dr. Joan Daemon and Dr. Vincet Rijmen from Belgium. Unlike DES, AES does not utilize a Feistel network. The AES algorithm is a symmetric key block cipher with length of block of 128 bits and backing for lengths of key of 128,192 and 256 bits. The AES algorithm is an algorithm of symmetric key which implies the same key is utilized to decrypt and encrypt a message. Additionally, the cipher text created by the AES algorithm is of the same size as the plain text message. The majority of the operations in the AES algorithm happen on bytes of data or on 4 bytes long data words, which are spoken to in the field GF (28), known as Galois Field. AES is in light of design principle called Substitution permutation network. AES works on a 4*4 matrix of bytes, which is termed as state. The cipher of AES is indicated as number of recurrences of transformation rounds that change over the input plain text into the last output of cipher text. Each round comprises of many steps of processing, including one that relies on the encryption key. Arrangements of reverse rounds are applied to change cipher text once again into the original plain text utilizing the same key of encryption. The AES algorithm circles through specific sections N_r times. It is fast in hardware and software. The steps in AES algorithm are as follows [4]:

1. Key Expansion: Round keys are gotten from the cipher key using Rijndaels's key plan.
2. Initial Round
a) Add Round Key: every state of the byte is added with the round key using bitwise XOR.
3. Rounds
a) Sub Bytes: a non linear step of substitution in which every byte is swapped with another as indicated by look up table.
b) Shift Rows: a step of transposition in which every row of the state is changed cyclically a specific number of steps.
c) Mix Columns: operation of mixing which works on the columns of the state, consolidating the four bytes in every column.
d) Add Round Key
4. Final Round (no Mix Columns)
a) Sub Bytes
b) Shift Rows
c) Add Round Key

III. GENETIC ALGORITHM

The genetic algorithm is a search algorithm depending on the procedure of natural genetics and natural selection. The genetic algorithm fits in with the group of evolutionary algorithms, alongside evolutionary programming, evolution strategies and genetic programming. The arrangement of operators generally contains selection, mutation and recombination. The principle idea is that in place for individual's population to adjust to some environment, it ought to act like characteristic framework. The reproduction and survival of an individual being is advanced by the end of pointless characteristics and by developing the valuable conduct. Genetic algorithms (GAs) consider a problem of optimization as the environment where possible solutions are the people living in that environment. The level of

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710
International Journal of Innovative Research in Science, Engineering and Technology
(An ISO 3297: 2007 Certified Organization)
Vol. 4, Issue 8, August 2015

adjustment of single person to its environment is the partner of the function of fitness assessed on a solution. Also, arrangement of practical solutions takes the spot of population of creatures. An individual is a string of binary digits or some other arrangement of symbols taken from a finite set. Every encoded individual in the population may be seen as representation of a specific answer for an issue. Generally, genetic algorithm starts with set of individuals that are generated randomly [5]. The pseudo code of genetic algorithm is as follows [6]:

- Select the individuals' initial population.
- Evaluate every individual's fitness in population.
- Repeat this procedure until condition of termination satisfied:
    - Selection: Select the individuals which are having greater fitness for reproduction.
    - Crossover: Breed new individuals through crossover.
    - Mutation: Apply probabilistic mutation on new individuals.
    - Form a new population with these offspring.
- Terminate

IV. RELATED WORK

Lots of Lots of research work has been done in the area of image security using cryptography techniques and genetic algorithms. Many methods have been proposed for security of images. Some important work in this area is as follows:

Reference [7] shows the design of 128 bit encoder for image encryption utilizing AES Rijndael algorithm. With the quick movement of exchange of data in the electronic way, security of information is getting to be more imperative in transmission and storage of data. Due to more utilization of images in process of industry, it is vital to protect the private data from unapproved access. The AES algorithm has been widely accepted. Timing simulation is also performed to confirm the usefulness of designed circuit.

In paper [8], authors use two techniques of security in steganography and cryptography. It is important to ensure the data while imparting over channels which are insecure. The two main branches of information security are cryptography and steganography. The matter of secret message is mixed in cryptography, where as in steganography the message which is secret is implanted into the cover medium. High security model is developed by consolidating security of cryptography and steganography. To encrypt secret image, AES is used. The encrypted image is secured with an alternate image by utilizing F5 algorithm.

In reference [9], authors use the techniques of steganography and cryptography with watermarking so that to secure the specific information. Steganography is proficient through concealing the information in some other information, along these lines by hiding the presence of conveyed information and steganography can be enhanced by joining it with the cryptography and watermarking. The fundamental idea of this proposed model is that it will permit a normal client to safely exchange the information by hiding them in file of digital image by using the local attributes inside the image, which will provide strong security.

Paper [10] introduces two methods where in steganography and cryptography are consolidated to encode the data and also to hide the data in an alternate medium through image processing. Steganography is the specialty of concealing the reality that communication is occurring. It do this by hiding data in some another data. Security of image by encryption is carried out by DES algorithm using the key image. The encoded image can be covered in some other image by utilizing techniques of LSB so that the existence of secrecy is covered. The decryption could be possible by same key image utilizing DES algorithm.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710
International Journal of Innovative Research in Science, Engineering and Technology
(An ISO 3297: 2007 Certified Organization)
Vol. 4, Issue 8, August 2015

V. MOTIVATION

The two main that arise in image encryption are with respect to time it takes for its computation and its security. For real time image encryption, only those ciphers are preferable which takes lesser amount of computational time without comprising security. Cryptography and steganography are two essential branches of information security. The purpose of both these is same but both are different. It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The main goal of this research is to do communication in a secure manner and also to avoid drawing suspicion to the transmission of hidden data.
The research is based on the following objectives:
1. To study various algorithms for data hiding and case study for the same.

2. To design and implement AES optimized with genetic algorithm to get higher PSNR and data hiding capacity.

3. To evaluate results with previously designed algorithms to predict the percentage of improvement.

VI. PROPOSED SCHEME

Cryptography and Steganography are the two main branches of the security of information. The main goal of the proposed system is to create a strong steganographic technique that can achieve high security and embedding capacity while maintaining image quality and imperceptibility. Step by step methodology is used in this work.
AES algorithm is a symmetric block cipher. It means we use the same key or may be single key for encryption and decryption. The algorithm is based on Rijndael algorithm which permits different block and key sizes. The size of block and key can be chosen independently from 128, 160, 192, 224, 256 and it is not compulsory to be the same. Many parameters of AES depend on the length of key. Likewise, if the size of key used is 128, then the number of rounds is 10 and it is 12 and 14 for 192 and 256 bits respectively. Every round instead of last one is a parallel and uniform composition of 4 steps:
1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

But AES algorithm is very difficult to implement because the usage of keys make it very complex and moreover it has very complex algebraic structure. If we use the keys then there are number of iterations which we have to implement in AES that make it very complex and also time consuming. So to overcome this difficulty, we have used genetic algorithm which is explained below:
1. Generate random population of *n* chromosomes (suitable solutions for the problem).
2. Evaluate the fitness *f(x)* of each chromosome x in the population.
3. Create a new population by repeating following steps until the new population is complete
   - Select two parent chromosomes from a population according to their fitness (the bigger fitness, the bigger chance to be selected).
   - With a crossover probability cross over the patterns to form a new offspring (children). If no crossover was performed, offspring is an exact copy of parents.
   - With a mutation probability mutate new offspring at each locus (position in chromosome).
   - Place new offspring in anew population.
4. Use generated population for a further run of algorithm.
5. If the end condition is satisfied, stop, and return the best solution in current population.

VII. EXPERIMENTAL RESULTS

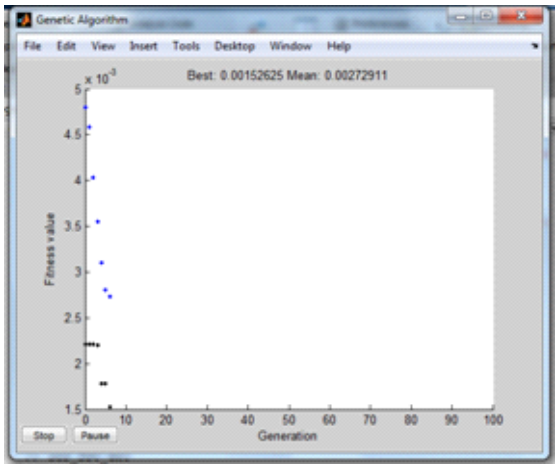
This section presents the simulation results of security of an image using AES and GA.

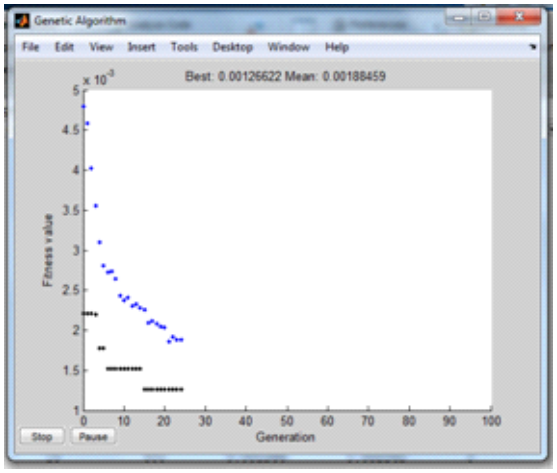
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

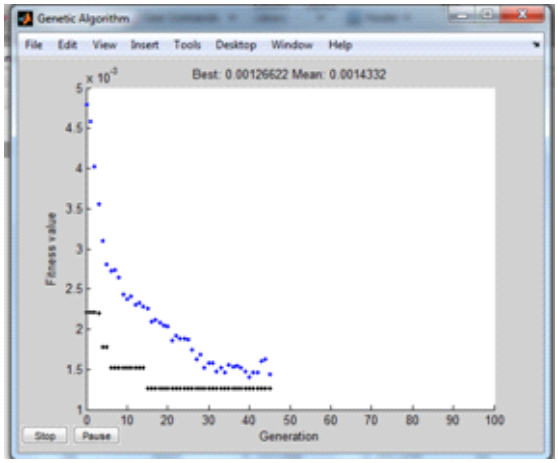
International Journal of Innovative Research in Science, Engineering and Technology

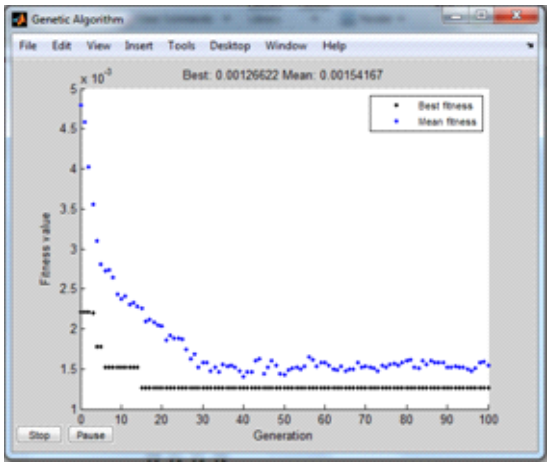
(An ISO 3297: 2007 Certified Organization)

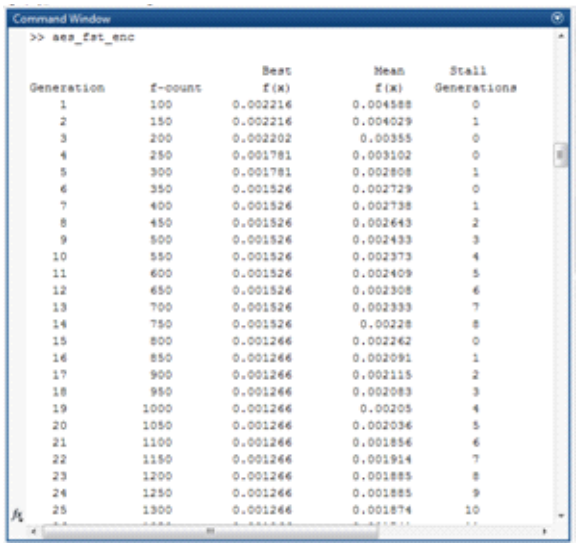
Vol. 4, Issue 8, August 2015





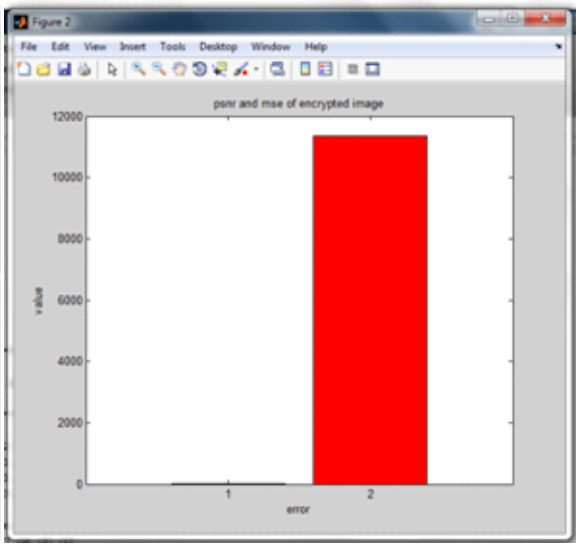






```
>> aes_fat_enc

                                  Best        Mean     Stall
Generation      f-count           f(x)        f(x)     Generations
     1            100          0.002216    0.004588       0
     2            150          0.002216    0.004029       1
     3            200          0.002202     0.00355       0
     4            250          0.001781    0.003102       0
     5            300          0.001781    0.002808       1
     6            350          0.001526    0.002729       0
     7            400          0.001526    0.002738       1
     8            450          0.001526    0.002643       2
     9            500          0.001526    0.002433       3
    10            550          0.001526    0.002373       4
    11            600          0.001526    0.002409       5
    12            650          0.001526    0.002308       6
    13            700          0.001526    0.002333       7
    14            750          0.001526     0.00228       8
    15            800          0.001266    0.002262       0
    16            850          0.001266    0.002091       1
    17            900          0.001266    0.002115       2
    18            950          0.001266    0.002083       3
    19           1000          0.001266     0.00205       4
    20           1050          0.001266    0.002036       5
    21           1100          0.001266    0.001856       6
    22           1150          0.001266    0.001914       7
    23           1200          0.001266    0.001885       8
    24           1250          0.001266    0.001885       9
    25           1300          0.001266    0.001874      10
```

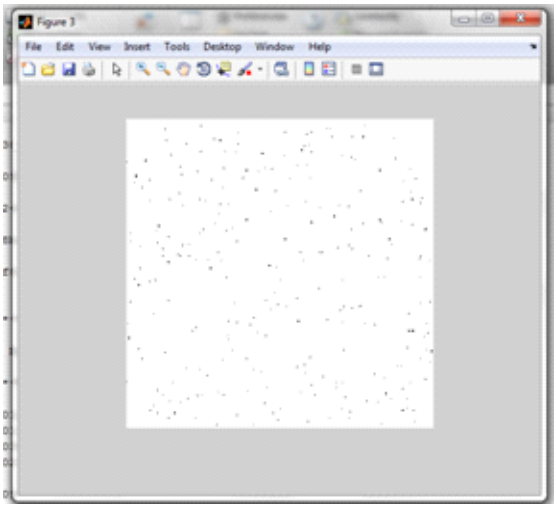


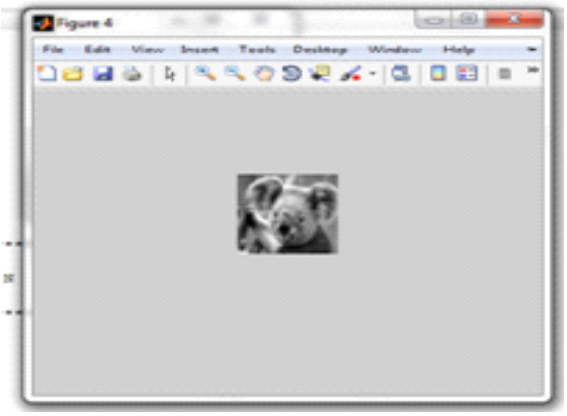
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

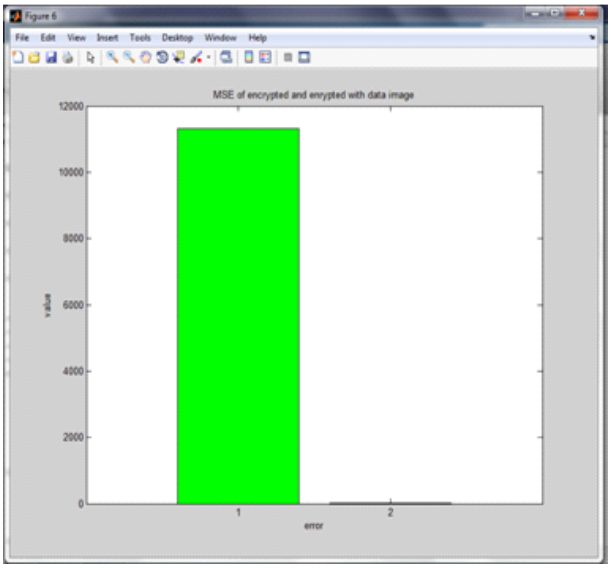
International Journal of Innovative Research in Science, Engineering and Technology

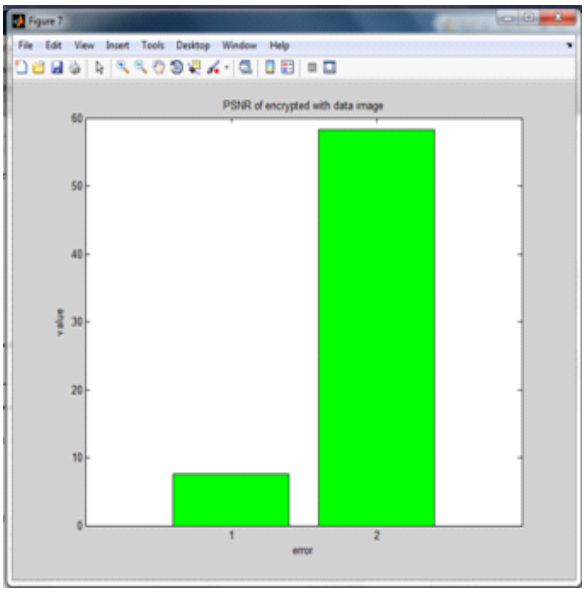
(An ISO 3297: 2007 Certified Organization)

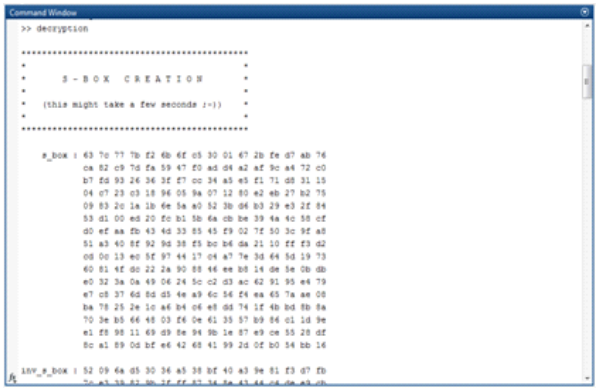
Vol. 4, Issue 8, August 2015

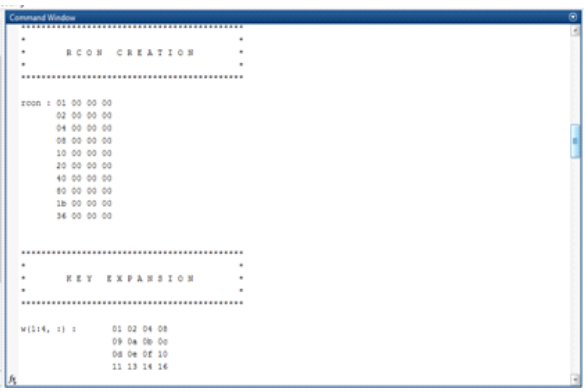










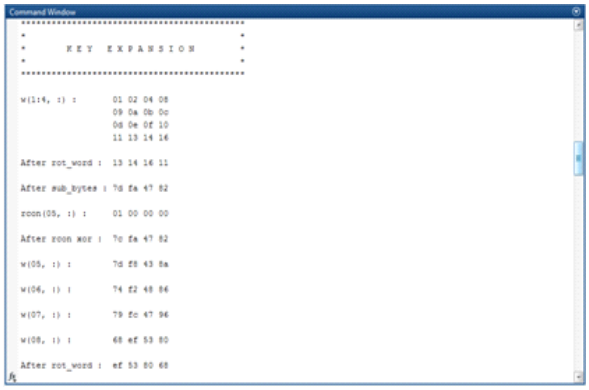


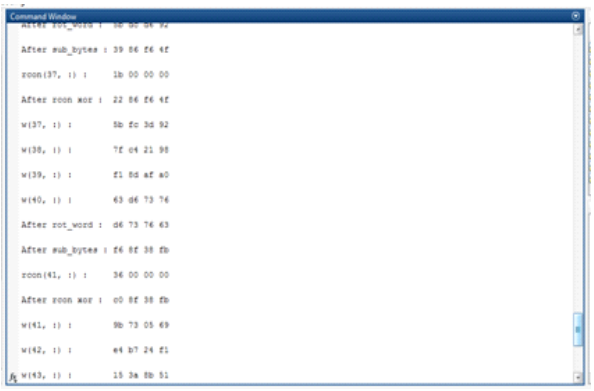
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

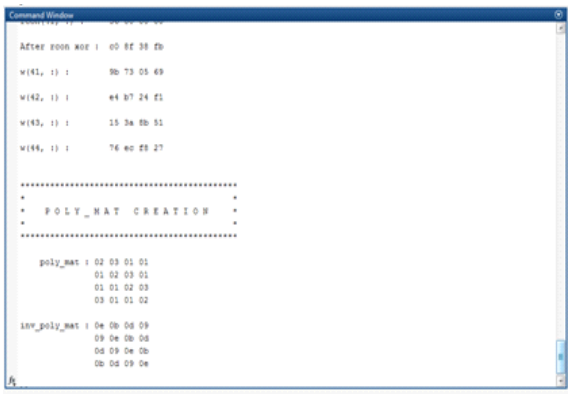
International Journal of Innovative Research in Science, Engineering and Technology

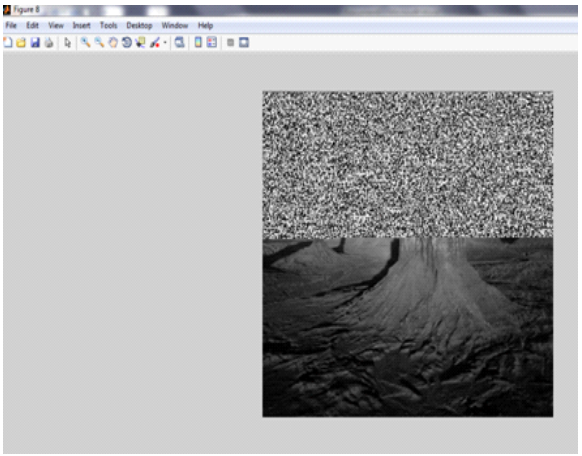
(An ISO 3297: 2007 Certified Organization)

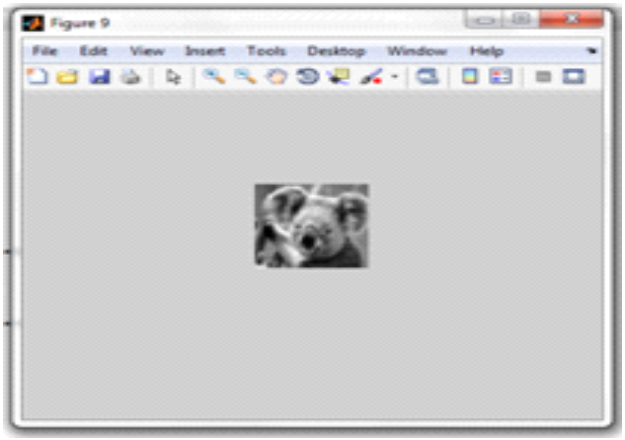
Vol. 4, Issue 8, August 2015











VIII. CONCLUSION

The main aim of this research work is to create a technique which is strong and steganographic and also which provides high security of information. This is done by implementing optimized AES and genetic algorithm to achieve higher PSNR and capacity of data hiding. The results obtained are compared with the previous algorithms and our technique provides better results.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

REFERENCES

1. Gamil R.S. Qaid, Sanjay N. Talbar, "Bit-Level Encryption and Decryption of Images Using Genetic Algorithm: A New Approach", IPASJ International Journal of Information Technology (IIJIT), Vol.1, Issue 6, December 2013.
2. Manoj Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, "Secured Steganography Approach Using AES", Intenational Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol.3, Issue 3, Aug 2013.
3. Ankita Aggarwal, "Security Enhancement Scheme for Image Steganography using S-DES Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 4, April 2012.
4. Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 4, April 2012.
5. Anil Kumar, M.K. Ghose, "Information Security using Genetic Algorithm and Chaos", Sikkim Manipal University of Technology, Sikkim.
6. Saif Hasan, Sagar Chordia, Rahul Varshneya, "Genetic Algorithm", Februray 2012
7. P.Karthigaikumar, Soumiya Rasheed, "Simulation of Image Encryption using AES Algorithm", IJCA Special Issue on "Computational Science-New Dimensions & Perspectives", NCCSE, 2011.
8. Sonu Varghese K, Faisal K K, Vinayachandran K K, "Image Security using F5 and AES Algorithm", Proceedings of IRF International Conference, Chennai, April 2014.
9. Sarita Poonia, Mamtesh Nokhwal, Ajay Shankar, "A Secure Image Based Steganography and Cryptography with Watermarking", International Journal of Emerging Science and Engineering (IJESE), Vol.1, Issue 8, June 2013.
10. R.Nivedhitha, Dr. T. Meyyappan, "Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology, Vol.3, Issue 3, 2012.
11. Ankita Aggarwal, "Secret Key Encryption Using Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol.2, Issue 4, April 2012.
12. Pye Pye Aung, Tun Min Naing, "A Novel Secure Combination Technique of Steganography and Cryptography", International Journal of Information Technology, Modeling and Computing (IJITMC), Vol.2 No. 1, Februray 2014.
13. Shamim Ahmed Laskar, Kattamanchi Hemachandran, "Secure Data Transmission Using Steganography and Encryption Technique" International Journal on Cryptography and Information Security (IJCIS), Vol.2, No. 3, September 2012
14. Jyotika Kapoor, Akshay. J. Baregar, "Security using Image Processing", International Journal of Managing Information Technology (IJMIT), Vol.5, No.2, May 2013.
15. Manoj. B, Manjula N Harihar, "Image Encryption and Decryption using AES", International Journal of Engineering and Advanced Technology (IJEAT), Vol.1, Issue 5, June 2012.
16. Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol.3, Issue 3,May-June 2014.
17. P. Radhadevi, P. Kalpana, Secure Image Encryption using AES", IJRET: International Journal of Research in Engineering and Technology, Vol. 1, Issue 2, Oct- 2012.
18.