INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Comparison between DES and AES hybridization with genetic technique for guarded image transmission

Shekharan Deep Bindra
bindra.shekharan5@gmail.com
Amritsar College of Engineering and Technology, Meharbanpur, Punjab

Navneet Bawa
bawa.navneet@gmail.com
Amritsar College of Engineering and Technology, Meharbanpur, Punjab

ABSTRACT

In this world of digital communication, data is the heart of the worldwide economy. The Paper is for a hybrid approach in which in which there is the implementation of cryptography for securing the images. The hybrid techniques are basically the merger of cryptography with stenography combined with a genetic algorithm. The working of both techniques is same but differs from each other. It is able to join the techniques to encrypt the text by deploying cryptography and then concealing the encrypted text by deploying Steganography. The idea behind in this analysis is to communicate in a protected way and to bypass the layout impression for the communication of concealed data which can manage high security and enclose the capacity to manipulate the image & imperceptibility.

Keywords: *Steganography, Cryptography, AES, Genetic techniques.*

1. INTRODUCTION

On arriving of the data communication & with other techniques of communication, the technologies like computerized transmission has become more popular to transact information, for example email, eBooks, websites, e-commerce, news, chat etc. but data sent in digital medium is an issue like verification, interference and protection of copyright. Now days an approach of encryption resolves these types of issues. The verification of data and detection of analog of digital image, audio and videos have caught devotion of the researchers. In earlier years, the research on image security focus on the problem for the security of copyrights, yet gave less consideration to speed, distortion and data loss. Every problem emerges the requirement for reliable techniques for encryption. [1]

1.2. TWO WAYS OF IMAGE SECURITY

1.2.1. Steganography: Steganography is basically an approach for masking the text in some another inoffensive digital media like image, video in manner that, it is tough for the individual to find the private message. For sharing the information that should be sent on other side securely we used steganography. [7] Some methods of Steganography join conventional Cryptography with Steganography; the sender encodes the confidential message preceding the whole process of communication, as it troubles a threat agent to distinguish the installed cipher message in a cover [10].

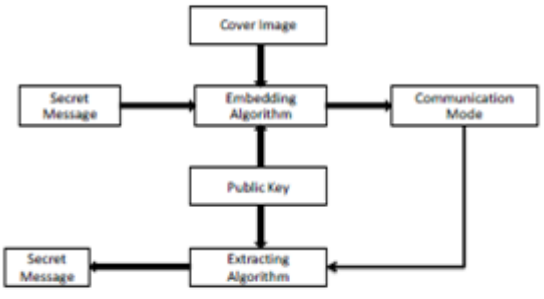


Fig 1: Basic layout of image Steganography [26]

Steganography is parted into three parts:

1) Pure Steganography

2) Secret Key

3) Public Key

1.2.2. Cryptography It masks the private messages information from the illegal individual which is yet to be visible. The method in which message structure is collected thus to make it insignificant and incomprehensible. Mostly, the technique cryptography endeavors the scope of addressing the content among the individual that preserves the stranger from reviewing it. [2]

Cryptography is of two types:

a) SYMMETRIC KEY

b) ASYMMETRIC KEY

1.3. STEGANOGRAPHY VS CRYPTOGRAPHY

Basically, an objective of both the techniques encipher the messages but still both are different. Cryptography masks the details of private message from unauthorized peoples, on another side steganography is for concealing the messages. The cryptography through which system gets crash when the malicious attacker tries or attempts to read the private message. For splitting steganography, the system demands an attacker to finds that steganography is been used. It is feasible to couple the two technologies to encrypt the messages using cryptography & then hides the encrypted content or message through steganography. The conclusion of stegno-image which will transmit after clarifying the information which is being changed.

2. METHODOLOGY

2.1. Existing methodology used:

The model of steganography works on DES functions that is permutation, substitution, S–Box mapping and secrete key.

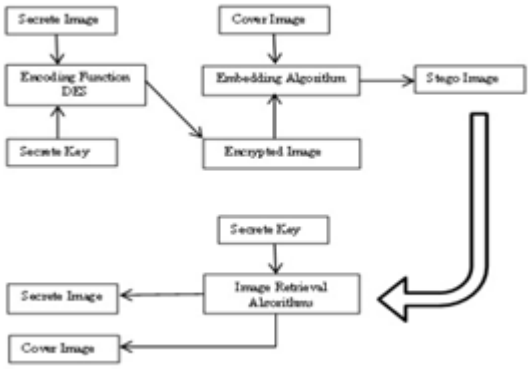
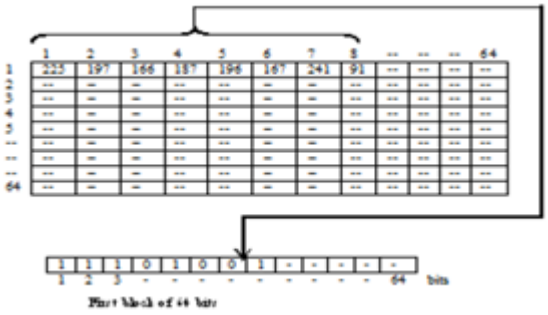


Figure: 2 Current miniature for steganography

A. Encoding Function

In this masked image is selected. The value of each pixel of masked image is converted from decimal to binary.



Figur3. Conversion of Decimal pixel value to Binary

Eight successive pixel values from secrete image form one block of 64 bits. DES encoding function is as below.

1) Initial / Inverse Initial permutation: The 64 – bit passes through an initial permutation (IP) that rearranges the bits to produce the 64-bit permutated output that input to phase consisting 16 round of same function (fk). The output of the sixteenth round will now input to reverse initial permutation by which the original ordering of the bits is restored.

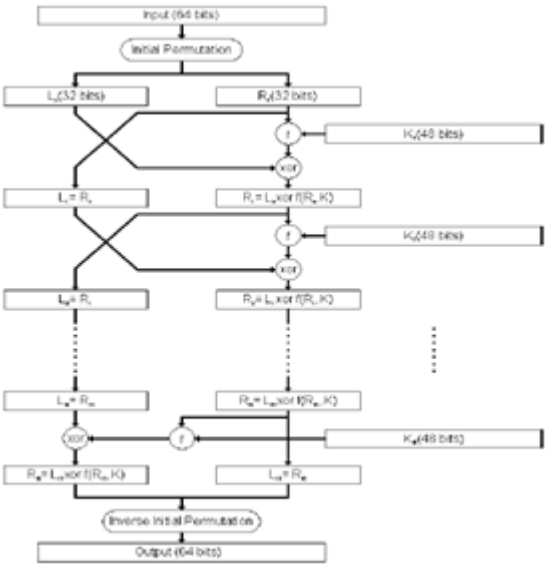


Figure 4. Encoding Function (DES) Detail

2) The function f: The difficult elemental for DES is function f. The function can be (typical)

Li = Ri-1,

Ri = Li-1 □ F (Ri-1, Ki)

3) S- box operation: It is composed of eight S-Boxes, each accepts 6 bits as input and produces 4 bits as an output. The first and last bits of input to box Si form a two-bit binary number to select one of four substitutions defined by four rows in the table for Si.

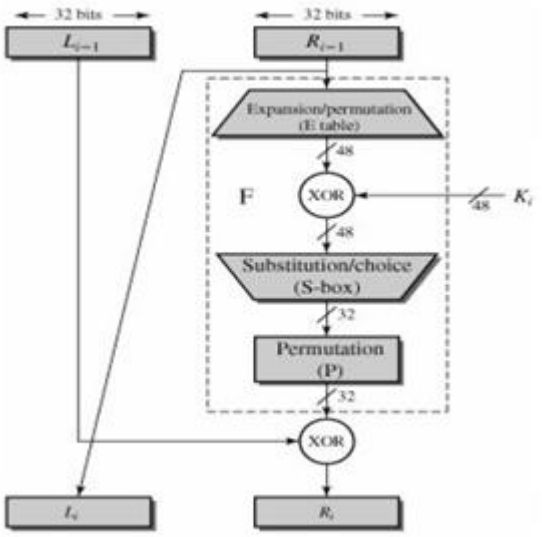


Figure 5. Single Round Detail

For example, in S1 for input 101011, the row is 11 (row 3) and the column is 0101 (column 5). The value in row 3, column 5 is 9, so the output is 1001.

S_1																
R/C	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Figure 6. S- Box Detail

One complete execution of DES gives the eight-pixel value of secrete image into respective pixel values of the encrypted secrete image.

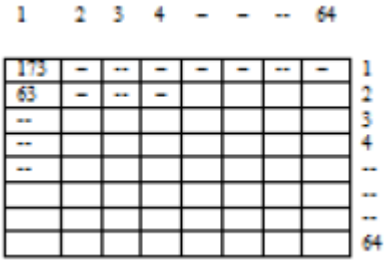


Figure 7. Hidden Secret Image (64 × 64)

4) Bit Division: Taking the encrypted image, the values are combined with decimal to binary. The binary value of

Next, divide this 8-bit value into 4 parts taking 2 bits in each

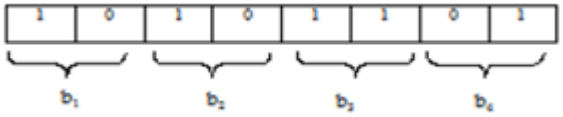


Figure 8. Bit Division

5) Insertion of Bit into the cover image: on receiving value for b1, b2, b3, b4, these values are inserted into the cover image. The pixels replaced by 10,10,11,01 in the cover image.

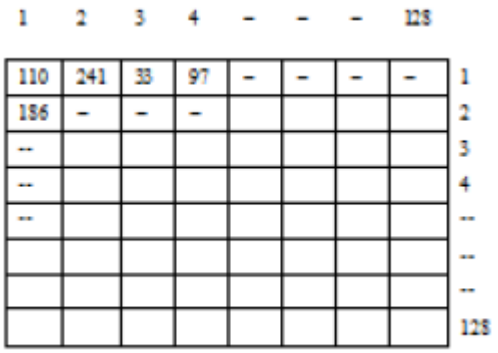


Figure 9. Cover Image (128 × 128)

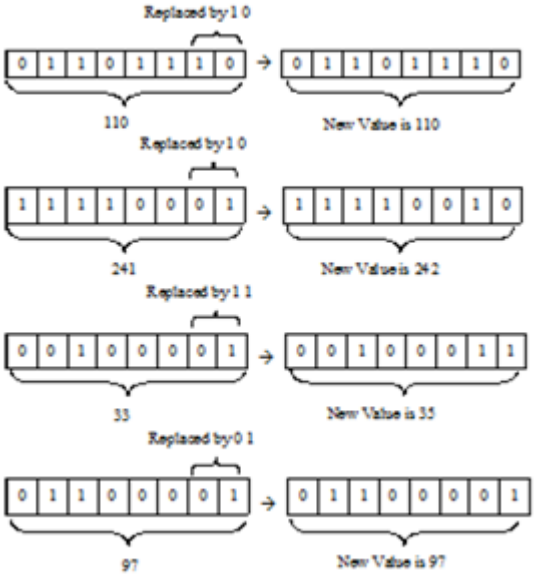


Figure 10. Insertion of Bit into Cover Image

6) Formation of Stego Image:

On accepting the pixel value, the stego image is formed by replacing these values at their original position.

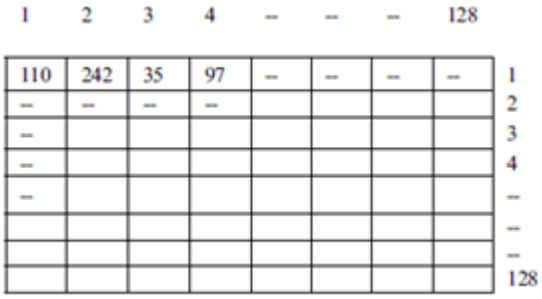


Figure 11. Creation of Stego Image (128 × 128)

• Encoding Algorithm:

Steps:

1) Input eight-pixel value of the secret image form block of 64 bits to the image encoding Function (DES), which produces the encrypted secrete image.

2) Divide each pixel value of encrypted secrete image into 4 parts containing 2 bits each.

3) Insert these pixel values into the LSB position of first four pixels in the cover image one by one.

4) End.

•Decoding Algorithm:

Input: Stego Image of size (2m × 2n);

Output: A gray level Secrete Image (m × n);

Steps:

1) Input each pixel and take 2-bit LSB from 4 consecutive pixel value of the stego image.

2) Concatenated four 2bit LSB get 8 bits of each pixel of the encrypted secrete image.

3) Now taking eight consecutive pixel value form block of 64 bits are input to decoding Function (DES) using same parameter but keys value used in reverse order getting the first eight-pixel value of secrete image.

4) End.

2.2. Proposed methodology used

The methodology used in my analysis is AES and Genetic technique which are explained as below:

AES (Advanced Encryption Standard): The method is established on Rijndael technique that charter blocks & key size. Advanced Encryption (AES) is an approach to iteration. Every emphasis (iteration) is called as round. Each round deal with one single byte which is based on substitution, the permutation step is row-wise, a mixing step which is column-wise & then there is a count of round key. The four conversions are as below:

• Sub Bytes: sub bytes work in every bite of state independently.

• Shift Row: shift row frequently moves the rows over singular offset.

• Mix Column: the mix columns taken as a polynomial over GF (2^8) and increases with an altered polynomial. It does not work on last round of AES technique.

Add Round key: it works on XOR operations.

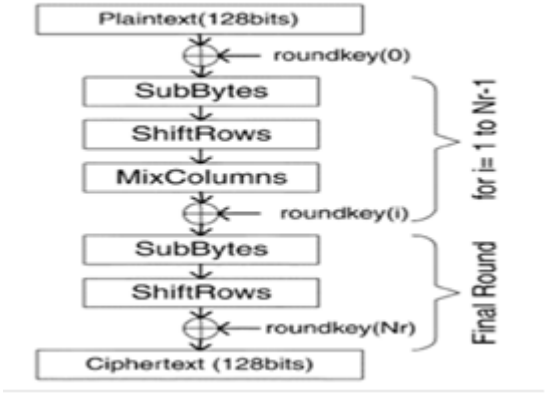


Figure 12- Block diagram of encryption part of AES

AES (Advanced Encryption Standard) is tough to deploy, the usages of key make it complex and if keys were used then there many iterations which we must deploy in AES which is time-consuming.

Genetic Algorithm: It is a searching technique on the procedure of natural selection. This is the optimized technique for the resolution of reported issues. The principle idea is that in place for individual's population to adjust to some environment, it ought to act like characteristic framework. The imitation and durability of being advanced at the end of pointless characteristics and by developing the valuable conduct.

1) [Start] – It Creates any unexpected population of n chromosomes

2) [Fitness] - Analyze the fitness that is f(x) of every chromosome.

3) [Population] - Generate the population by imitating the below steps until completion of new population Select two parent chromosomes from a population

a. [Selection] on the selection of two main chromosome in a population to give their fitness (the larger fitness, the larger change to be accepted).

b. [Crossover] with the crossover the chances of cross over the marking to create a new children (offspring). Otherwise, offspring performed a copy of parents.

c. [Mutation] with the mutation there is chances to modify a newly created offspring at every locus.

d. [Accepting] newly created offspring is placed on new population.

Place new offspring in a new population.

4) [Replace] Use created a population for a further run in the algo.

5) [Test] on the satisfaction of result, stop and gave the best result in the current population.

2.3. RESULTS OF PROPOSED METHODOLOGY:

This section presents the simulation results of we have obtained of security of image using AES and Genetic Algorithm.

Part 1: Encryption

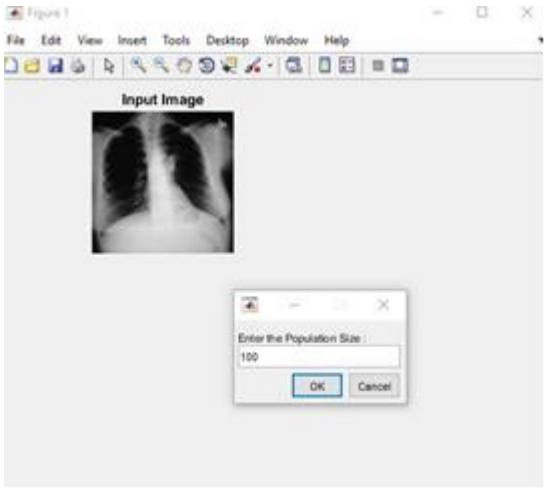


Figure: 13 select the user-defined image to insert size of population for genetic technique

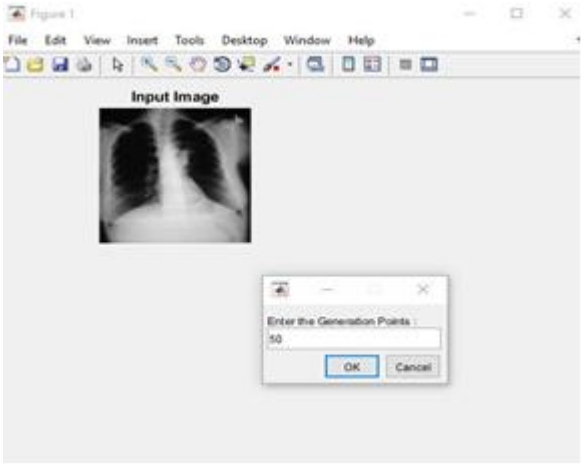


Figure: 14 in this enter generation point for genetics

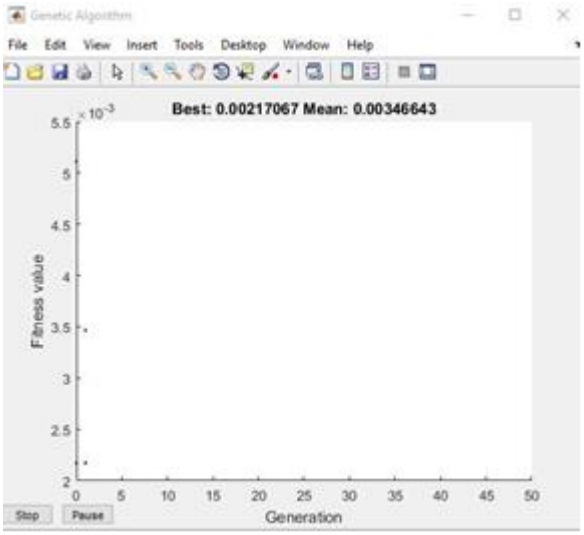


Figure: 15 Generation point vs fitness value Plot to show the best value at 2 Generation points

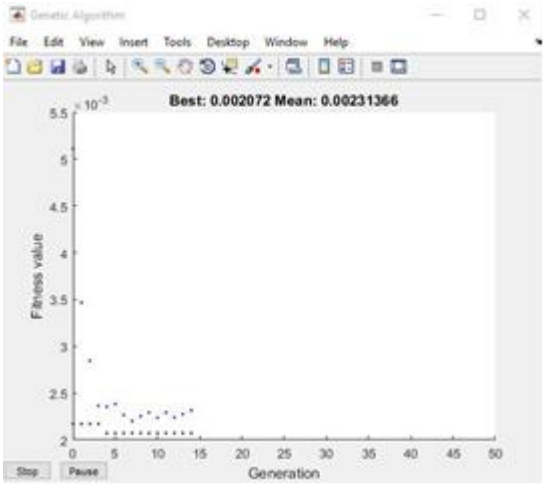


Figure: 16 Fitness value vs Generation point plot to show the best value at 14 Generation points

Showing all the values of Generation Points, f-count Best and mean value for 25 Generation Points.

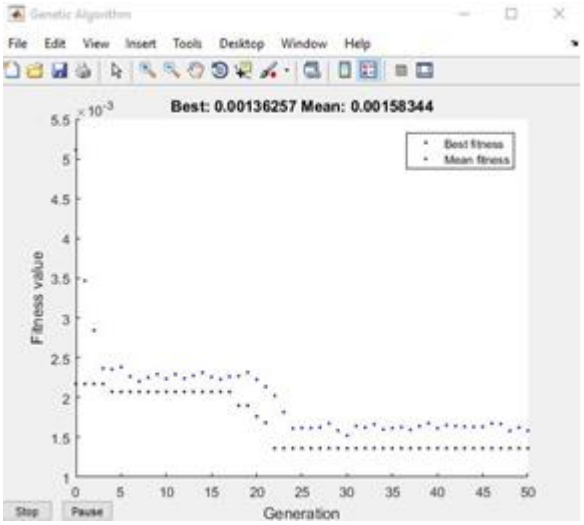


Figure: 17 Fitness Value v/s Generation point plot to show the best value at 50 Generation points

The final value in a pattern of PSNR, MSE Maxerr, L2Rat and Total Encryption Time

```
psnr1 =

    7.5115

mse1 =

   1.1533e+04

maxerr =

   248

l2rat =

    1.2598

Total_encryption_Time =

  458.2015
```

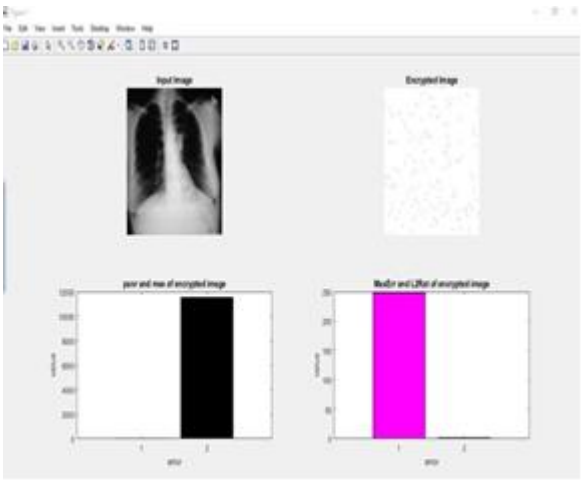


Figure: 18 Show Entered (Input) image and encrypted Image with results values in bar graphs.

Part-2 Data Hiding

In this, I entered the message which I want to hide in the input image.

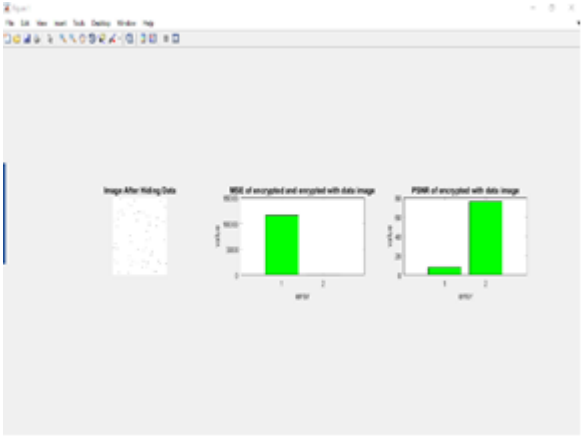


Figure: 19 Shows Image after Data Hiding and shows results in bar graphs

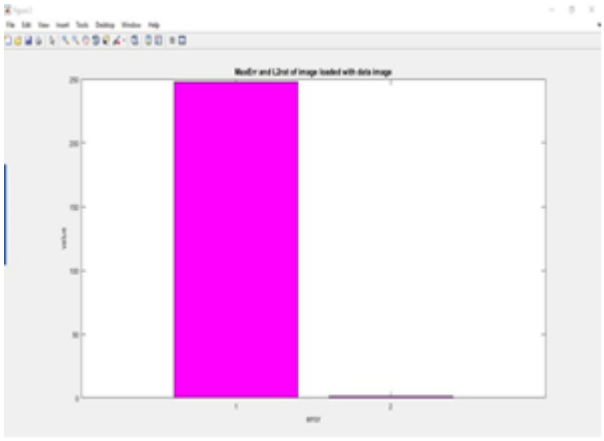
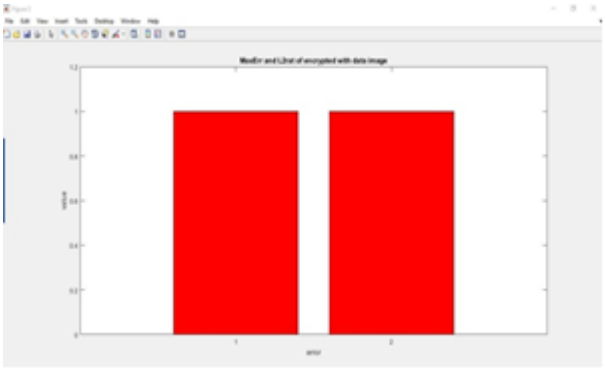


Figure: 20 MaxErr and L2rat Value results create Bar Graph between Input Image and Image after data hiding



MaxErr and L2rat Value results make a Bar Graph between Encrypted Image and Image after data hiding.

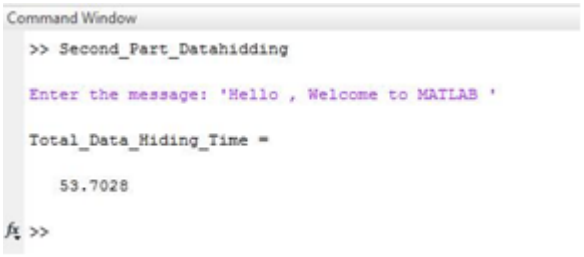


Figure: 21 shows time taken by the system to mask the data in the image

Part-3 Decryption

```
>> Third_Part_Decryption

*****************************************
*                                       *
*      S-BOX  CREATION                  *
*                                       *
*   (this might take a few seconds :-))  *
*                                       *
*****************************************

    s_box : 63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe d7 ab 76
            ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c a4 72 c0
            b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 d8 31 15
            04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 27 b2 75
            09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 2f 84
            53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c 58 cf
            d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 3c 9f a8
            51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff f3 d2
            cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 5d 19 73
            60 81 4f dc 22 2a 90 88 46 ee b8 14 de 5e 0b db
            e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e4 79
            e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea 65 7a ae 08
            ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 8b 8a
            70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 c1 1d 9e
            e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce 55 28 df
            8c a1 89 0d bf e6 42 68 41 99 2d 0f b0 54 bb 16
```

```
inv_s_box : 52 09 6a d5 30 36 a5 38 bf 40 a3 9e 81 f3 d7 fb
            7c e3 39 82 9b 2f ff 87 34 8e 43 44 c4 de e9 cb
            54 7b 94 32 a6 c2 23 3d ee 4c 95 0b 42 fa c3 4e
            08 2e a1 66 28 d9 24 b2 76 5b a2 49 6d 8b d1 25
            72 f8 f6 64 86 68 98 16 d4 a4 5c cc 5d 65 b6 92
            6c 70 48 50 fd ed b9 da 5e 15 46 57 a7 8d 9d 84
            90 d8 ab 00 8c bc d3 0a f7 e4 58 05 b8 b3 45 06
            d0 2c 1e 8f ca 3f 0f 02 c1 af bd 03 01 13 8a 6b
            3a 91 11 41 4f 67 dc ea 97 f2 cf ce f0 b4 e6 73
            96 ac 74 22 e7 ad 35 85 e2 f9 37 e8 1c 75 df 6e
            47 f1 1a 71 1d 29 c5 89 6f b7 62 0e aa 18 be 1b
            fc 56 3e 4b c6 d2 79 20 9a db c0 fe 78 cd 5a f4
            1f dd a8 33 88 07 c7 31 b1 12 10 59 27 80 ec 5f
            60 51 7f a9 19 b5 4a 0d 2d e5 7a 9f 93 c9 9c ef
            a0 e0 3b 4d ae 2a f5 b0 c8 eb bb 3c 83 53 99 61
            17 2b 04 7e ba 77 d6 26 e1 69 14 63 55 21 0c 7d
```

S-Box and Inverse S-Box Matrix created while performing decryption.

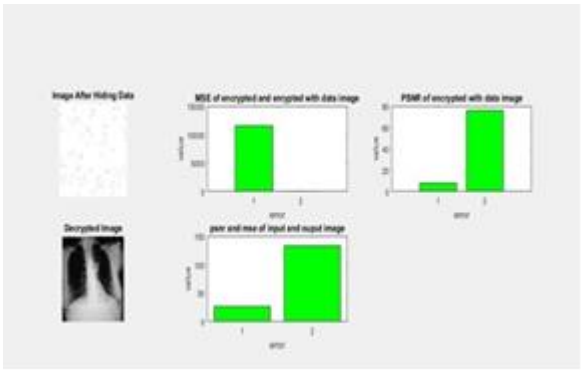


Figure: 22 Shows Input image after data hiding and decrypted image with result values in bar graphs

```
recieved_msg =

'Hello , Welcome to MATLAB '


Total_Decryption_Time =

  109.6640
```

It shows time taken by the system to decrypt the image.

3. CONCLUSION

Our focus is to create a technique which is strong and steganographic and to provide high security of information. This is possible by optimizing AES and Genetic Algorithm to achieve higher PSNR value and capacity of data hiding. Steganography when joined cryptography is a wonderful tool which enables for secret communication.

4. FUTURE SCOPE

Steganography has gained extensive importance with the growth of new technologies and internet. The available methods focus on the strategy of embedding and give no concentration to the stages of pre-processing, these methods may be combined for MPEG formats so that more secure transmission can be done.

5. 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] Shamim Ahmed Laskar, KattamanchiHemachandran, "Secure Data Transmission Using Steganography and Encryption Technique", International Journal on Cryptography and Information Security (IJCIS), Vol. 2, No. 3, September 2012.
[3] Ramesh Gottipati, "Audio-Based Security System with Image Steganography", International Journal of Software Engineering and Technology Informatics, Vol. 1, Issue 1, January 2015.
[4] ManojRamaiya, Naveen Hemrajani, Anil Kishore Saxena, "Secured Steganography Approach Using AES", Vol. 3, Issue 3, August 2013.
[5] DiptiKapoorSarmah, NehaBajpai, "Proposed System for data hiding using Cryptography and Steganography", Department of Computer Engineering, Maharashtra Academy of Engineering, Pune, India.
[6] R.Nivedhitha, Dr.T.Meyyappan, "Image Security Using Steganography and Cryptographic Techniques", International Journal of Engineering Trends and Technology, Vol. 3, Issue 3, 2012.
[7] YojnaGoyal, Manmohan Sharma, "Proposed AES for Image Steganography in Different Medias", International Journal of Research in Engineering and Technology, Vol. 3, Issue 10, October 2014.
[8] ShrikhandeRohini, VinayakBairagi, "Lossless Medical Image Security", International Journal of Applied Engineering Research, Dindigul, Vol. 1, No. 3, 2010.
[9] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, Vol. 1, No. 15, 2010.
[10] AlaaTaqa, A.A Zaidan, B.B Zaidan, "New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm", International Journal of Computer and Electrical Engineering, Vol. 1, No. 5, December 2009.
[11] B.G. Priyanka, S.V. Sathyanarayana, "A steganographic system for embedding image and encrypted text", International Conference on Contemporary Computing and Informatics (IC3I), November 2014.
[12] S.H. Kamali, R. Shakerian, M. Hedayati, M. Rahmani, "A new modified version of Advanced Encryption Standard based algorithm for image encryption", International Conference on Electronics and Information Engineering (ICEIE), Vol. 1, August 2010.
[13] P.Karthigaikumar, SoumiyaRasheed, "Simulation of Image Encryption using AES algorithm", IJCA Special Issue on Computational Science- New Dimensions & Perspectives", NCCSE, 2011.
[14] Sonu Varghese K, Faisal K K, Vinayachandran K K, "Image Security using F5 and AES algorithm", Proceedings of IRF International Conference, 13 April-2014, Chennai, India.
[15] PyePyeAung, 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, February 2014.
[16] Hussein Al-Bahadili, "A Secure Block Permutation Image Steganography Algorithm", International Journal on Cryptography and Information Security (IJCIS), Vol. 3, No. 3, Spetember 2013.
[17] JyotikaKapur, Akshay. J. Baregar, "Security using Image processing", International Journal of Managing Information Technology (IJMIT), Vol. 5, No. 2, May 2013.
[18] M.Zeghid, M.Machhout, L.Khriji, A. Baganne, R.Tourki, "A Modified AES Based Algorithm for Image Encryption", International Journal of Computer, Control, Quantam, and Information Engineering, Vol. 1, No. 3, 2007.
[19] 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.
[20] Manojgowtham.G.V, Senthur. T, Sivasankaran. M, Vikram.M, "AES Based Steganography", International Journal of Application or Innovation in Engineering and Management (IJAIEM), Vol. 2, Issue 1, January 2013.
[21] RinkiPakshwar, Vijay Kumar Trivedi, VineetRichhariya, "A Survey on Different Image Encryption and Decryption Techniques", International Journal of Computer Science and Information Technologies, Vol. 4(1), pp. 113-116, 2013.
[22] AnkitaAggarwal, "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.
[23] ShubhanginiP.Nichat, Prof. Mrs.S.S. Sikchi, "Image Encryption using Hybrid Genetic Algorithm", International Journal of Advanced Research on Computer Science and Software Engineering, Vol. 3, Issue 1, January 2013.
[24] Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptographic Technique", International Journal of SdvancedResaerch in Computer Science and Software Engineering, Vol. 2, Issue 4, April 2012.
[25] AnkitaAggarwal, "Secret Key Encryption Algorithm Using Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 4, April 2012.
[26] SaritaPoonia, MamteshNokhwal, Ajay Shankar, "A Secure Image Based Steganography and Cryptography with Watermarking", International Journal of Emerging Science and Engineering (IJESE), Vol. 1, Issue 8, June 2103.
[27] KavehAhmadi, MaralMohamadiZanjani, "A New Method for Image Security and Data Hiding in Image", International Conference on Business, Economics and Tourism Management (IPEDR), Vol. 24, 2011.
[28] Mona F.M,Mursi, HossamEldinH.Ahmed, Fathi E. Abd El-samie, AymanH.Abd El-aziem, "Image Security with Different Techniques of Cryptography and Coding: A Survey", Recent Advances in Electrical and Computer Engineering
[29] Mohammad SajidQamruddinKhizrai, Prof. S.T.Bodhke, "Image Encryption using Different Techniques for High Security Transmission over a Network", International Journal of Engineering Research and General Science, Vol. 2, Issue 4, July 2014.
[30] P.Radhadevi, P.Kalpana, "Secure Image Encryption using AES", International Journal of Research in Engineering and Technology, Vol. 1, Issue 2, October 2012.

[31] Ramaiya M. K., Hemrajani N. and Saxena A. K. "Security Improvisation in Image Steganography using DES", 3rd IEEE Trans. International Conference IACC -2013, Page(s): 1094 – 1099. 2013
[32] Ramaiya M. K., Hemrajani N. and Saxena A. K., "Security Improvisation in image Steganography applying DES", International Conference on Communication Systems and Network Technologies, IEEE Page(s): 431-436. 2013
[33] PHILJON T. L. J AND VENKATESHVARA R. N. "METAMORPHIC CRYPTOGRAPHY -A PARADOX BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY USING DYNAMIC ENCRYPTION", IEEE-INTERNATIONAL CONFERENCE RECENT TRENDS IN INFORMATION TECHNOLOGY, ICRTIT 2011

