INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY
IJARIIT
ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 5 - V7I5-1346)
Available online at: https://www.ijariit.com

DES and AES hybridization by the genetic process of image transfer by comparison

Gaurav Arora
gauravarora0207@gmail.com
Mewar University, Gangarar, Rajasthan

ABSTRACT

Hybrid paper in which there is the use of cryptography to protect images. Hybrid techniques are basically a combination of cryptography and steganography integrated with a genetic algorithm. The effectiveness of the two methods is the same but different from each other. It can join encryption techniques by installing cryptography and hide encrypted text by sending Steganography. The idea of this analysis is to communicate in a secure manner and to go beyond the confines of confidential communications that can handle high security and enable image handling and anonymity.

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

1. INTRODUCTION

With the advent of data communication and other communication strategies, technologies such as computer transfers have become increasingly popular for data processing, for example email, eBooks, websites, e-commerce, news, chat etc. issue as a guarantee, interference and copyright protection. Nowadays the encryption method solves these kinds of problems. Data verification and analogue acquisition of digital image, audio and video hold the researchers' commitment. In previous years, image security research focused on copyright security issues, but provided little attention to acceleration, distortion and data loss. Every problem arises from the need for reliable encryption techniques. [1]

1.2. Two ways of image security

1.2.1.Steganography: Steganography is basically a way to hide text in other non-annoying digital media such as a photo, video in such a way, it is difficult for a person to get a private message. By sharing information that should be sent to the other party safely we have used steganography. [7] Other forms of Steganography include Standard Cryptography and Steganography; the sender enters the encryption code that precedes the entire communication process, as it disturbs the threat agent to isolate the encrypted message on the cover [10].

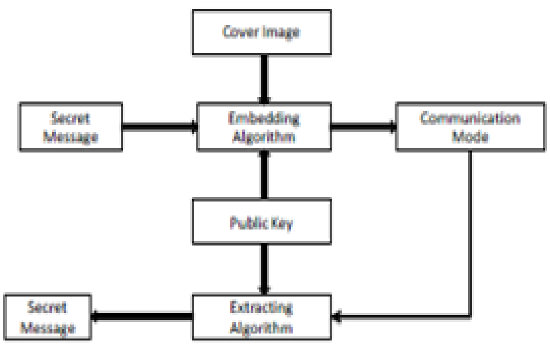


Figure 1: Basic editing of the image Steganography [26]

Steganography is divided into three sections:
1) Pure Steganography
2) Secret Key
3) Public Key

Cryptography hides the details of a private message from an illegal person who is yet to be identified. The way in which the structure of the message is collected is therefore insignificant and incomprehensible. Most importantly, the cryptography writing process attempts to address content within the person that keeps the stranger in the review. [2] Cryptography is of two types:

a) Symmetric key
b) Asymmetric key

1.3. Steganography vs Cryptography

Basically, the purpose of both methods is to insert messages but both are different. Cryptography hides the details of private messages from unauthorized persons, while steganography is for encryption. Cryptography in which the system crashes where a malicious attacker tries or tries to read a secret message. By separating steganography, the system requires the attacker to find out if steganography is being used. It is possible to pair two encryption technologies using cryptography and hide encrypted content or message via steganography. The end of the stegno image that will pass after specifying the changing details.

2. METHODOLOGY

2.1. Existing methodology used

The steganography model works on DES permutation functions, replacement, S-Box map and secrete key.

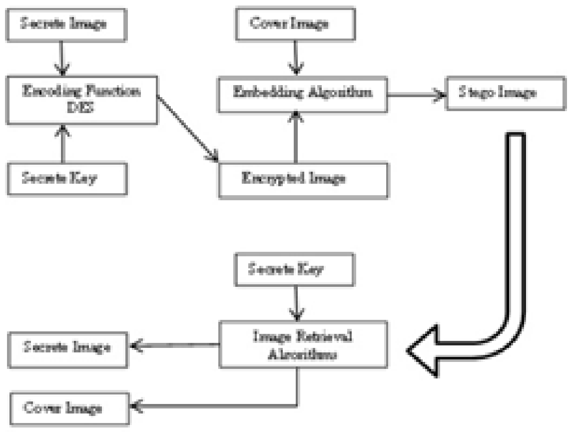


Figure: 2 The current miniature of steganography

A. Encoding Function

This hidden image has been selected. The pixel value of each hidden image is converted from decimal to binary.

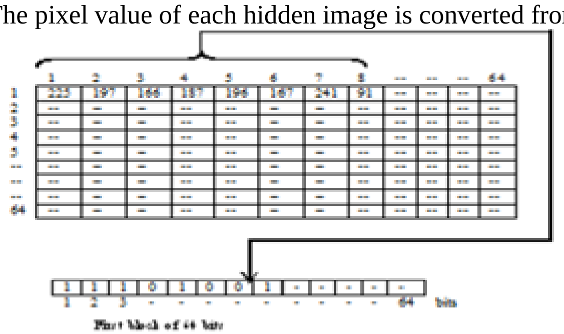


Figure 3. Conversion of a decimal pixel value to Binary

The value of eight consecutive pixels from a private image from a single block of 64 bits. The DES encoding function is below. Initial Permit / Incoming Permit: 64 - bit passes through the original Permit (IP) which rearranges the fragments to produce a valid 64-bit output output included in a category containing 16 cycles of the same function (fk). The issuance of the sixteenth cycle will now be included to reverse the original permit where the actual return of the bits is restored.

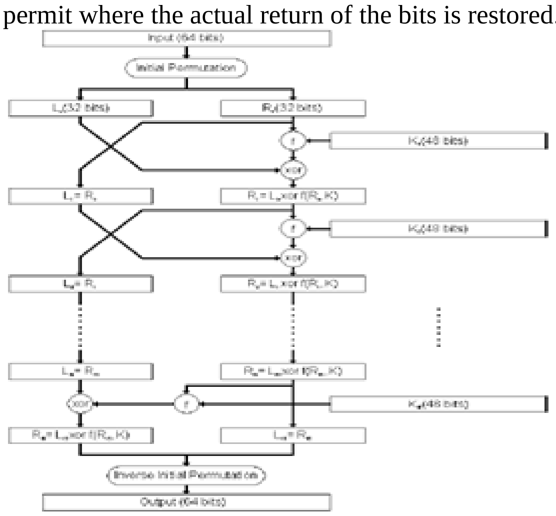


Figure 4. Function for encoding (DES) Details

1) TActivity *f*: The complexity of DES function *f*. Work can be (typical) Li = Ri-1,

Ri = Li-1 F (Ri-1, Ki)

2) S-box performance: Made up of eight S-Boxes, each receiving six bits as an insert and producing 4 pieces as an outlet. The first and last bits of input Si form a binary number with two bits to select one of the four inputs defined by four lines in Si's table.

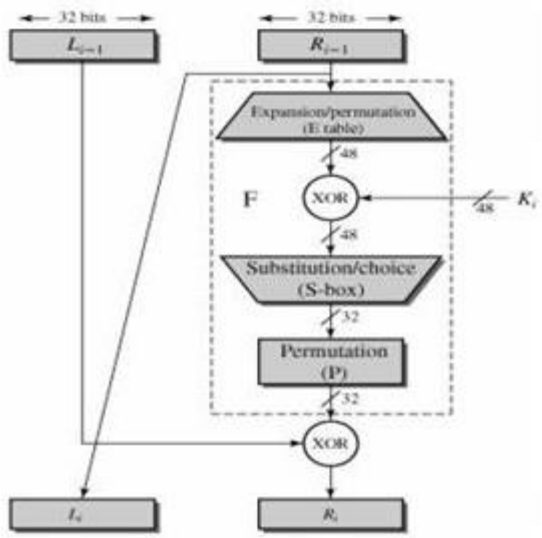


Figure 5. Single Round Detail

3) 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. Detail of S- Box One complete execution of DES gives the eight-pixel value of a secret image into respective pixel values of the encrypted secret image

1	2	3	4	–	–	--	64	
173	–	--	–	–	–	--	–	1
63	–	--	–					2
--								3
--								4
--								--
								--
								--
								64

Figure 7. Secret Image (64 × 64) (Hidden)

4) Bit Division: Taking the encrypted image, the values are combined from decimal to binary. The binary value of Next, divide this 8-bit value into 4 parts taking 2 bits in each

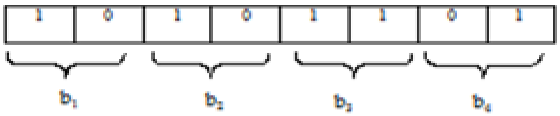


Figure 8. Bit by bit division

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

1	2	3	4	–	–	–	128	
110	241	33	97	–	–	–	–	1
186	–	–	–					2
--								3
--								4
--								--
								--
								--
								128

Figure 9. Cover Image (128 × 128)

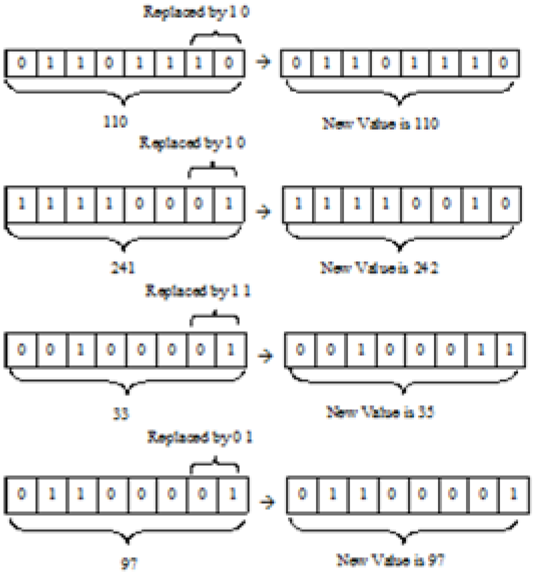


Figure 10. Image of insertion of Bit into a cover image

6) Formation of Stego Image:

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

1	2	3	4	–	–	–	128	
110	242	35	97	–	–	–	–	1
–	–	–	–					2
–								3
–								4
–								–
								–
								–
								128

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

- **Encoding Algorithm:**

Steps:

1) Enter a total of eight pixels of the 64-bit encrypted image form block in the image encoding (DES) action, which produces an encrypted private image.
2) Divide each pixel value of encrypted secret image into four parts containing 2 bit each.
3) Insert these pixels into the LSB of the first four pixels on the cover image one by one.
4) End.

- **Decoding Algorithm:**

Enter: Stego Image size (2m × 2n);

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

1) Insert each pixel and take 2-bit LSB from 4 consecutive pixel value of stego image.
2) The four combined 2bit LSB roots get 8 pieces of each pixel of encrypted secret image.
3) Now take the form of a consecutive 64 pixel pixel form to complete the task (DES) using the same parameter but the key value used to undo to get the first eight pixels of image encryption.
4) End.

2.2. Proposed methodology used

The method used in my analysis is the AES and genetic technique described below:

AES (Advanced Encryption Standard): This method is based on the Rijndael process for base blocks and key sizes. Advanced Encryption (AES) is a duplicate method. All iterations are called a circle. Each cycle works with one single byte based on replacement, smart approval step, smart mix step with column and then count of circular keys. Four modifications below:

- Sub Bytes: sub bytes run in all parts of the state independently.
- Shift Line: The switch line usually moves more than one offset line.
- Combine Column: Mixing columns were considered polynomial over GF (2 ^ 8) and multiplied by converted polynomial. It does not apply to the final round of the AES method.

Enter the round key: apply to XOR operations.

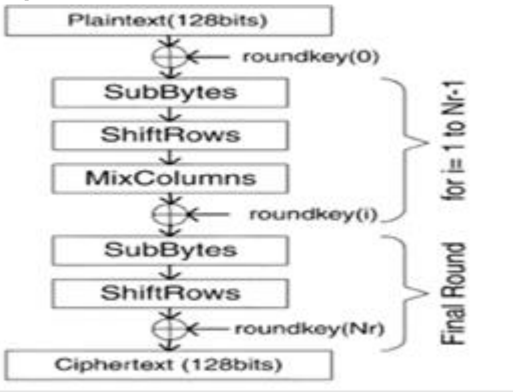


Figure 12- Block diagram of encryption part of AES

AES (Advanced Encryption Standard) is difficult to use, the use of keys makes it complicated and if the keys were used then there are many methods we have to use in AES that are time consuming.

Genetic Algorithm: It is a way of thinking about the process of natural selection. This is a process designed to solve reported problems. The basic premise is that instead of human beings agreeing with a particular place, it should serve as a feature framework. Imitation and firmness of progress in the end of unimaginable features and in developing important character.

1) [Start] –It creates any unexpected number of chromosomes
2) [Fitness] - Analyze the f (x) compatibility of all chromosomes.
3) [Population] -Generate a population by following the steps below until the number of young people is selected Select two parent chromosomes from humans
   a. [Selection] is the selection of two social chromosomes to provide their durability (greater durability, greater change to be adopted).
   b. [Crossover] and crossover opportunity to cross the mark to create a new child (interest). Besides, the interest made a copy of the parents.
   c. [Genetic mutation] has the potential to alter the newly created genetics everywhere.
   d. [Acceptance] The newly created interest is placed on young people. Put new interest on young people
4) [Replace] The application created a number of people to move forward on the algo.
5) [Check] for satisfaction of the result, stop and give the best result to the people present.

2.3. Results of methodology

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

Part 1: Encryption

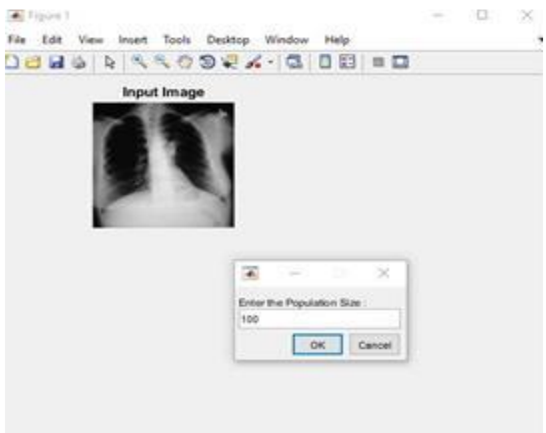


Figure: 13 select a user-defined image to enter the genetic technique

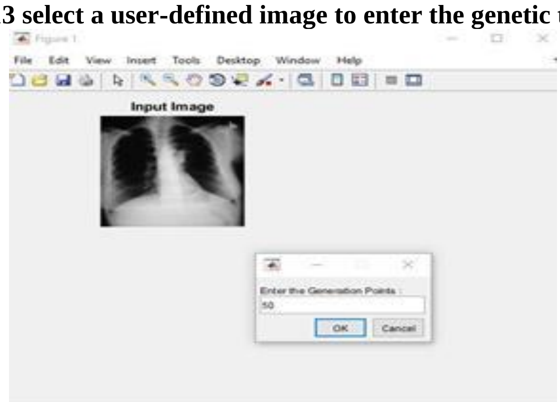


Figure: 14 at this point of inclusion of this gene generation

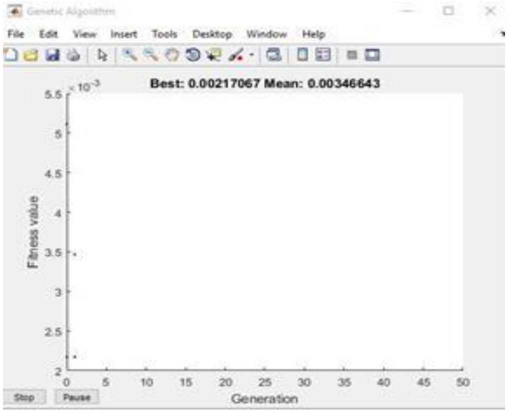


Figure: 15 Generation point vs richness value to show the best value of 2 Generation points

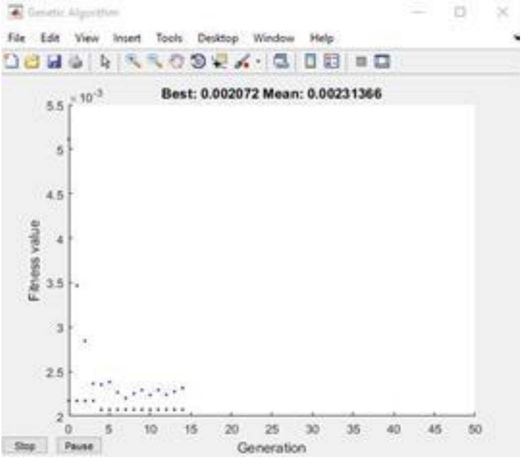


Figure: 16 Value strength vs Generation generation point to show the best value of 14 Generation point

Displays all Generation Points values, f-count Best and mean value of 25 Generation Points.

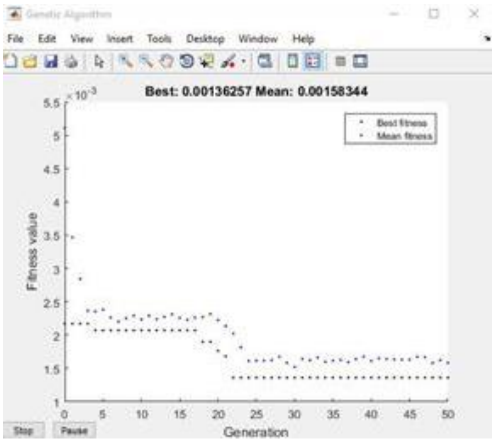


Figure: 17 Fitness Value v / s Generation point structure to show the best value of 50 Generation points

Final value for PSNR pattern, MSE Maxerr, L2Rat and full encryption time

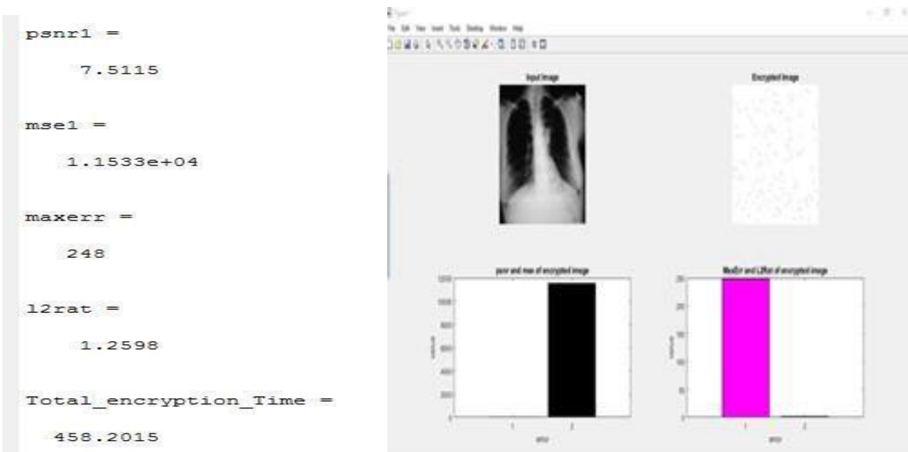
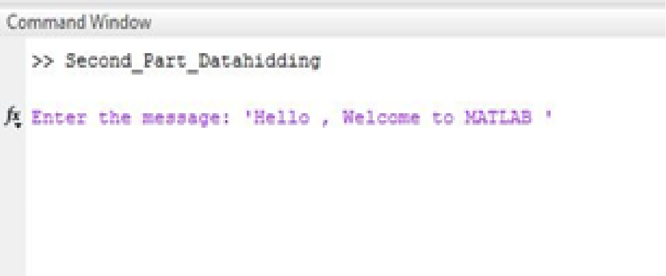


Figure: 18 Show the input (Input) a picture and an enclosed image with the effect values on the bar graphs.

Part-2 Hiding Data



In this case, I inserted a message I want to hide in the input image.

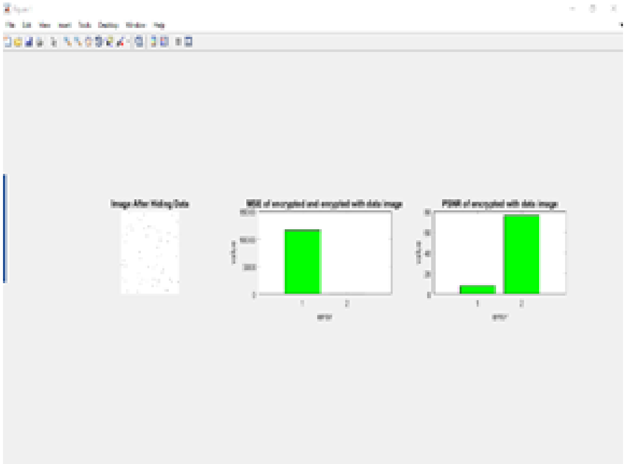


Figure: 19 Displays Image after encryption and shows results on bar graphs

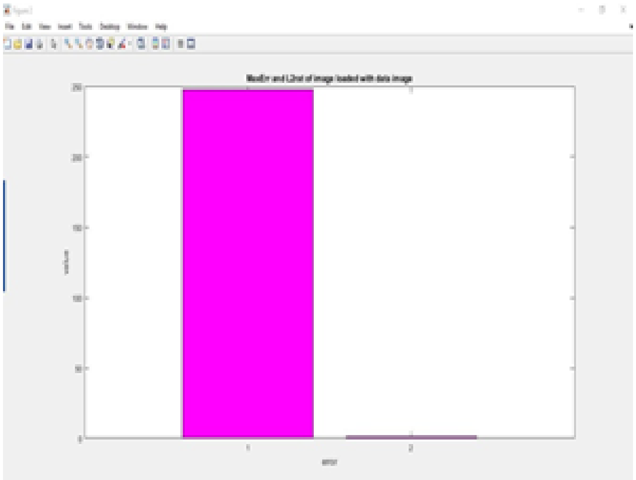


Figure: 20 MaxErr and L2rat Value results create a Bar Graph between Input Image and Image after hiding data

MaxErr and L2rat Value effects create a Bar Graph between encrypted image and image after data hiding.

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

Part-3 Decryption

```
>> Third_Part_Decryption

*******************************************
*                                         *
*      S - B O X   C R E A T I O N        *
*                                         *
*   (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
```

The S-Box and Inverse S-Box Matrix were created during encryption.

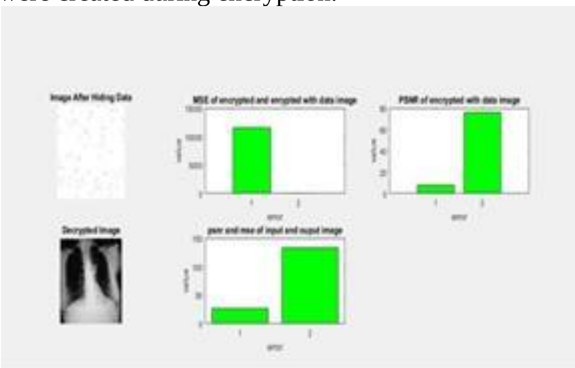


Figure: 22 Shows input image after encrypting data and encryption image with result values on bar graphs

```
recieved_msg =

'Hello , Welcome to MATLAB '


Total_Decryption_Time =

  109.6640
```

Indicates the time taken by the system to clear image encryption.

3. CONCLUSION

Our focus is to create a robust and steganographic process and provide high information security. This is possible by increasing AES and Genetic Algorithms to achieve higher PSNR value and data encryption capabilities. Steganography when combined with cryptography is a great tool that enables confidential communication.

4. FUTURE SCOPE

Steganography has gained tremendous growth with the growth of new technologies and the internet. The available methods focus on embedding strategy and do not provide focus on pre-processing stages; these methods can be integrated with MPEG formats for secure transfers.

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. 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
[31] 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
[32] 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

