A Secured System for Information Hiding in Image Steganography using Genetic Algorithm and Cryptography

Pratiksha Sethi
Dept. of Information & technology
Institute of Engineering and Technology
Devi Ahilya Vishwa Vidhyalaya, Indore

V. Kapoor
Dept. of Information & Technology
Institute of Engineering and Technology
Devi Ahilya Vishwa Vidhyalaya, Indore

ABSTRACT
Encryption is used to securely communicate data in open networks. Each type of data has its own structures; therefore according to the data the different techniques should be used to defend confidential data. Among them digital images are also very popular to carry confidential information in untrusted networks. . For pleasing the defense of data hiding and communication over network, the proposed system uses cryptographic algorithm along with Steganography. In the proposed system, the file which user want to make secure is firstly compressed to shrink in size and then the compressed data is altered into cipher text by using AES cryptographic algorithm and then the encrypted data is concealed in the image. In order to hide the information over the image in complex manner the genetic algorithm based technique is implemented which is used to evaluate the valuable pixels where the data can be hide in a secure manner. In addition of that, for hiding the information in images, the LSB (least significant bits) based steganographic method is used after the selection of eligible pixels. The implementation of the anticipated technique is performed using JAVA technology and for performance evaluation the time and space complexity is computed. In addition of that a comparative study of the proposed technique using the image steganographic technique is also performed in terms of PSNR and MSE. According to the computed performance the proposed technique is adoptable for hiding information in image securely additionally that consumes less space complexity.

General Terms
Image Steganography, Genetic Algorithm, Cryptography.

Keywords
Steganography, AES cryptographic algorithm, LSB, genetic algorithm.

1. INTRODUCTION
These days internet is used for more rapidly transmission of huge volume of essential and valuable data. Due to this, it is susceptible to many kinds of attack, so this information needs to be endangered from unauthorized access and the other privacy and security issues. To defend data from illegal access there are many data protection techniques like Nulling Out, Watermarking, Masking Data and Cryptography etc. are implemented [1]. Among these techniques the Cryptography and the Steganography is a classical approach of data security. In cryptography the data is transformed into an unreadable format during encryption process and during decryption data is again recovered in its original format. On the other hand in data steganography the data is encapsulated in a specific format of multimedia files to hide the sensitive information and during the recovery of data the information is retrieved from its original format without any modification on its cover. Steganography and cryptography are techniques used to shelter information from unwanted parties but neither technique alone is perfect. Once the actuality of hidden information is publicized or suspected, the reason of Steganography is somewhat defeated. The asset of Steganography increases by combining it with cryptography [2].

In this work the recommended system practices both cryptography and steganography for enhanced privacy and security. Even if these modus operandi are merged directly, there is a chance that the intruder may discriminate the original message. Therefore, here we applied both of them together with more security levels to get a very highly secured system for data hiding. In the proposed system to thwart the influence of Steganalysis method, Genetic Algorithm is used for pixel selection of image where data is to be hide so that finding of clandestine information become multifarious.

In image steganography the image facts is used to obscure the data, the data that has to be hidden can be an image, text or other sensitive or private information that is required to pass on in untrustworthy environment. Therefore the proposed system offer a pioneering method that hide different formats of data in intention image. This is accomplished by electing the pixels and incorporates data on it. Therefore for electing the optimum pixels in a given image for concealing data, the feature selection technique can help. Thus the proposed technique comprises the implementation of the soft computing based method namely genetic algorithm, which is used to elect the best possible pixels for incorporating the data. Since genetic algorithm is a heuristic established technique. Therefore fewer alterations are required in the conventional genetic algorithm for direct pixel selection [3]. By applying genetic algorithms the method will become computationally unviable to break. Genetic algorithms are a domestic of computational prototypes belonging to the class of heuristic evolutionary algorithms.

The main aim of the proposed work is to improve the stenographic data strength by incorporate the soft-computing facet in the data feature assortment [3].

2. LITERATURE SUMMERY
2.1 Cryptography
The progression of altering the data into scribbled format is called cryptography. It does not only defends data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic techniques usually used to achieve these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and

hybrid cryptography, each of which is described below. In each technique, the original data is called as plaintext. It is encrypted into cipher text by applying encryption algorithms, and on the receiver end the cipher text is decrypted into original plaintext [4].

2.1.1 Classification of Cryptography

Cryptography can be distributed into three major categories based on the use of key [5].

2.1.1.1 Symmetric Cryptography

In this type of cryptography identical key is used for encryption and decryption process. The key sharing has to be made before the communication of the information starts. The key plays a very vital role in this kind of encryption. Example: DES, BLOWFISH, AES etc. [6].

2.1.1.2 Asymmetric Cryptography

In this type of cryptography different keys are used for encryption and decryption process. Two different keys are generated at once and one key is dispersed to other side before the transmission starts. Asymmetric encryption is the contrary of symmetric encryption in security, since it doesn't involve sharing the secret key between the sender and the receiver. Any message (binary files, text or documents) that are encrypted by via public key can solitary be decrypted by applying the same algorithm, but by using the corresponding private key and vice versa. A disadvantage with asymmetric encryption yet, is that it is sluggish than symmetric encryption. It involves far more processing control to both encrypt and decrypt the message. Example: RSA algorithm.

2.1.1.3 Hybrid Cryptography

Hybrid cryptography is an approach of encryption that joins two or more encryption systems. It integrates a combination of symmetric and asymmetric encryption to benefit from the powers of each form of encryption. These strengths are respectively defined as speed and security. Hybrid cryptography is considered as highly secured type of encryption as long as the public and private keys are fully secured [7].

2.2 Steganography

Steganography is a skill of concealing the fact with the purpose of secured communication, by hiding information in other digital media like image, audio and video information. In steganography, many different carrier file formats are used now days, but the digital images are most popular for hiding information because of their frequency on Internet [8].

2.2.1 Image Steganography

In the image Steganography the information is hidden absolutely in images. The Image Steganography has been categorized into two [9].

2.2.1.1 Spatial domain Steganography:

It primarily comprises LSB Steganography and Bit Plane Complexity Slicing (BPS) algorithm [11, 12]. Spatial domain is frequently used because of its high capability of hiding information and easy realization.

2.2.1.2 Transform domain Steganography

The secret information is embedded in the transform coefficients of the cover image. Examples of transform domain Steganography are Discrete Cosine Transform, Discrete Fourier Transform and Discrete Wavelet Transform. [10]

Least Significant Bit (LSB) Based Steganography:

Like other techniques, this technique also implants the data into the cover image so that it cannot be noticed by the usual human vision. In LSB technique, the data embedding is possible on any bit of the image, but it is performed on preferably least significant bits. The bits of every pixel of the image are used and this method is important for using a loose less compression to protect the hidden information. The LSB technique generally uses three bits from every pixel (represented with 24 bits) where bits of the secret data are stored to hide secret data in the image [13].

3. PROPOSED WORK

The given Figure1 shows the proposed working model for image steganography. The components of the proposed model are described as:

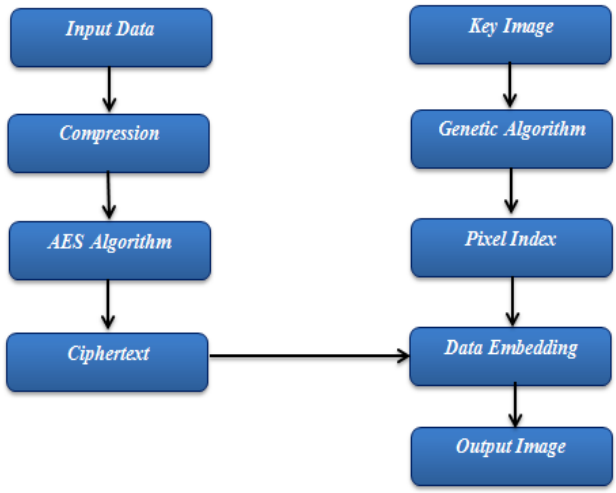

Figure 1 Proposed Model

Input Data: It is the information or message which is required to hide from the attackers. The foreseen system works on or selects any file as input to the system that can be in any format (text, image, docs, etc.) but need to compare the data size to be hide because the large data on small image cannot be hidden.

Compression: The input file is first compressed using the compression algorithm or using the ZIP utility. This reduces the size of original data which is required to hide in a given key image.

AES Algorithm: This algorithm specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The input, the output and the cipher key for Rijndael are each bit sequences containing 128, 192 or 256 bits with the constraint that the input and output sequences have the same length. The length of the input and output sequences can be any of the three allowed values but for the AES the only length allowed is 128.

Cipher Text: It is the produced cipher text after applying AES algorithm, the data is treated again in this phase. Therefore initially the whole data is converted into a four bit fixed blocks, which is used to replace the key image recovered bits of the pixels. Thus the substitution of LSB is performed on the basis of four bit.

Key Image: The key image is the image which is used to hide the sensitive data. Therefore that can be used in any size

depends upon the amount of data that is required to hide in image.

Genetic Algorithm: The genetic algorithm usage the three main phases first selection, cross over and mutation. [14]. But the involved operators are usages the random selection process for searching the key data. Therefore the recovery of original data which is hidden in image is suspected. Thus need to add some heuristics during selection process to obtain the fixed set of pixels by evaluation of row and column pixels [3].

Objective function is used when someone uses Genetic Algorithm to optimize the parameters of system or in complex search process. The area of interest here is to perform uniform single point crossover to generate complex cipher. Therefore here no objective function is used.

Modification on Genetic Algorithm: Firstly the image is treated in the row manner and used for data embedding. If the data remains to hide thus the process hide data in column based manner. Therefore the images of M X N are used and the selection of random rows of solution is used with the threshold input, in the following manner:

Input: threshold T, number of row pixels N

Process:

1. Select row N*T index
2. Remove selected index and resize the image
3. Again count index = N*T
4. Remove selected index and resize the image
5. Selected index rows are cross over first by which new image row generated
6. Find the low intensity pixel form selected sequences.
7. Embed data on pixels

Pixel Index: In this stage the selected pixels are used to conceal the data. Thus the selected pixels indices provide reference for algorithm processing.

Data Embedding: The embedded pixels of data is stored separately in a two dimensional vector to recover the output image.

Output Image: This is the finally generated image with hidden data and can be used for transmission in network.

The combined algorithm process of the proposed genetic algorithm based image steganography is given using table 1.

Table 1 Proposed Algorithm

Input: input text IT, threshold T, Key image K, cryptographic key K_e Output: encrypted data I_e
Process: 1. $R = readData(IT)$ 2. $Z = ZipCompress(R)$ 3. $CT = AES.encrypt(Z, K_e)$ 4. $[Row, Col] = ReadImage(K)$ 5. $I_e^i = InitilizeArray(Row, Col)$ 6. $for(i = 1; i \leq Row; i++)$ a. $POP = [Row, Col]$ b. $Sel_{index} = Row_i * T$ c. $POP = Resize(Row - Row_i)$ d. $Sel2_{index} = Row_i * T$ e. $POP = Resize(Row - Row_i)$ f. $SEQ[2] = CrossOver(Sel_{index}, Sel2_{index})$ g. $Sel_{Pixel}[\ ] = IsLowIntensity(SEQ[2])$ h. $I_e^i = EmbedData(Sel_{Pixel}, CT, SEQ[2])$ 7. end for 8. return I_e

4. APPLICATION OF THE PROPOSED TECHNIQUE

A simulation environment is employed as ImageSteganography using Net Beans IDE 8.0.2 (Integrated Development Environment).An application of the proposed algorithm with a test image (back.jpg) has been shown in Figures (2, 3, and 4). Figures show a carrier image/key image (back.jpg), a secret /input file (traditionalGA.text) and after steganography the corresponding stegano image as Encrypted image respectively. Figure 2 shows the selection of an input file which user want to hide. Figure 3 shows the selection of input key image in which user want to hide the input file. Figure 4 shows the stganoImage after applying proposed algorithm and Figure 5 shows the decoding process for getting the original file back. Here the stganoImage shows very least changes in the original image which cannot be easily identified by naked human eyes. On decoding the secret file (traditionalGA.text) is obtained back

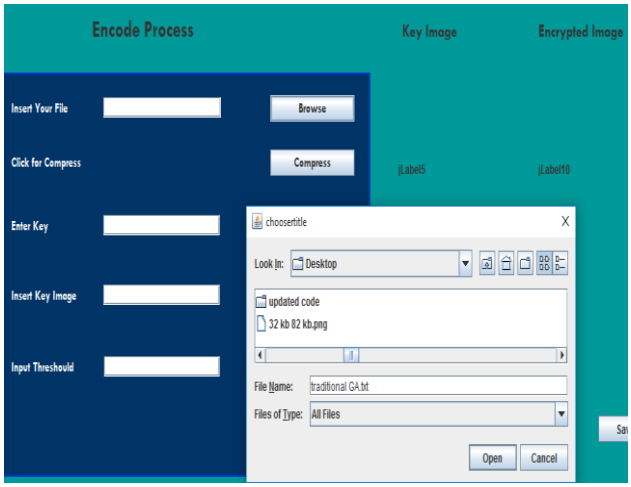

Figure 2 Selection of input/secret file (traditionalGA.text*)*

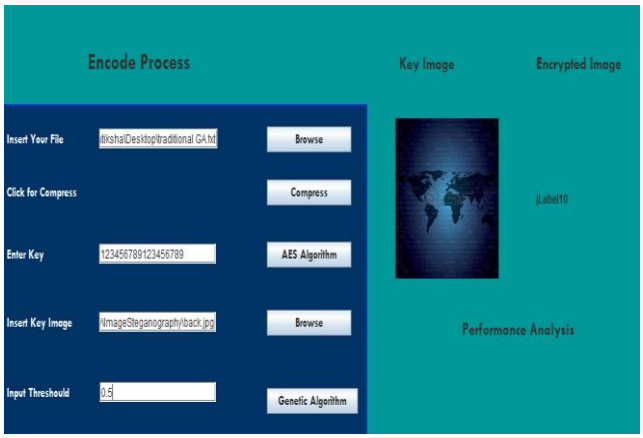

Figure 3 Selection of input key image (back.jpg)/before steganography

Figure 4 StganoImage/Encrypted Image after steganography

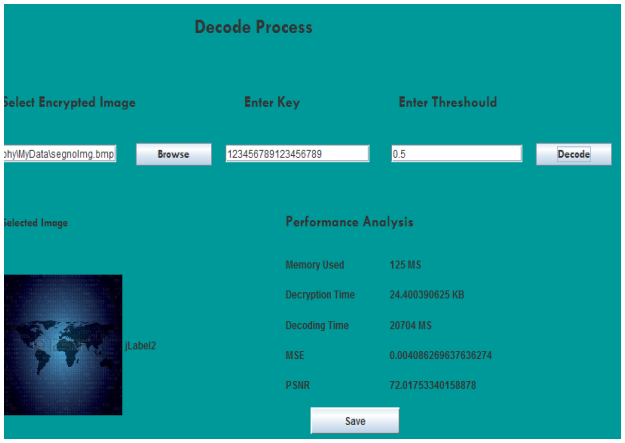

Figure 5 Decoding process

5. RESULT ANALYSIS

To give more potential about the performance of the proposed algorithm, this section talk over the results with different parameters:

5.1 Encryption Space Complexity

Space complexity is a measure of the quantity of working storage (main memory) an algorithm requires. That means how much memory, in the worst case, is needed at any point in the algorithm. Encryption Space Complexity of an algorithm is total amount of space consumed by the algorithm to encrypt the file with respect to the input size. Space complexity take in both Auxiliary space and space used by input file. The space complexity of the proposed system is given using figure 3. In order to demonstrate the performance of proposed algorithm the X-axis illustrates the different experiments performed with the system (file size in KB) and the Y-axis contains the memory consumption of the system in terms of KB. According to the obtained results the performance of the proposed algorithm is found efficient.

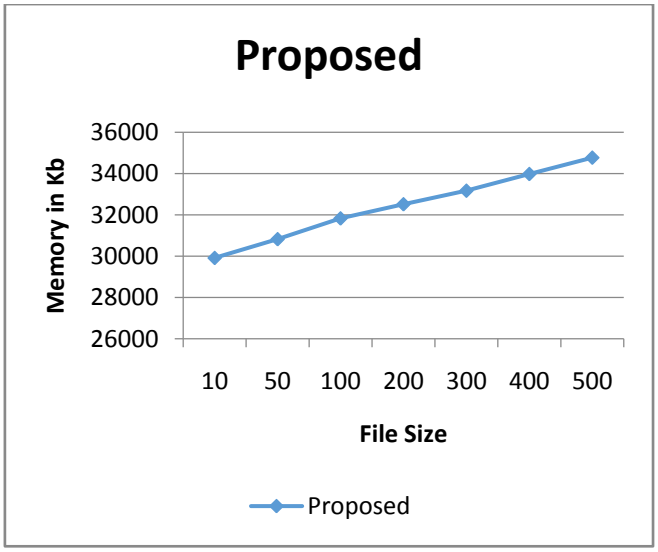

Figure 6 Encryption Space Complexity

5.2 Encryption Time

The amount of time required to encrypt the file using the selected algorithm is termed as the encryption time. The comparative encryption time of the proposed algorithm is given using figure 4. In this diagram the X-axis shows the file size of experimental set in terms of KB and the Y-axis contains the time consumed in terms of seconds.

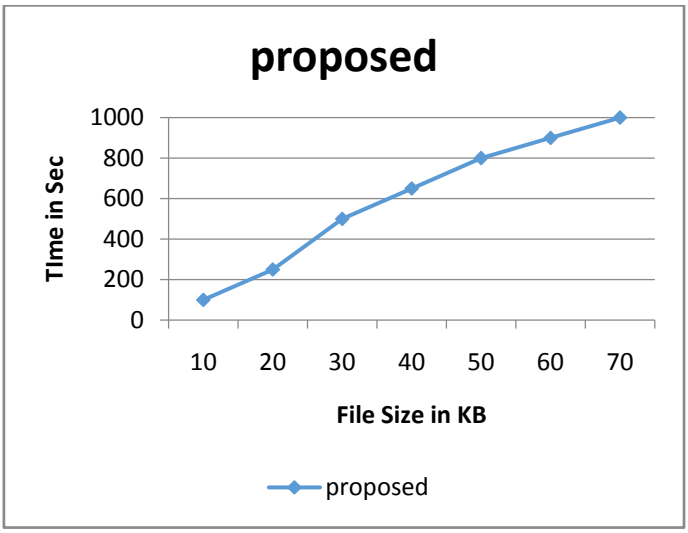

Figure 7 Encryption Time

According to the obtained results the proposed algorithm consumes significant amount of time. Therefore in near future it is required to enhance the algorithm for improving the time complexity of algorithm.

5.3 Decryption Time

Decryption is the process of transforming encrypted data again into its original form, so it can be understood. Encryption and decryption should not be confused with encoding and decoding, in which data is transformed from one form to another but is not intentionally altered so as to obscure its content. The amount of time required to decrypt the file using the selected algorithm is known as the decryption time. The performance of the proposed algorithm is given using figure 5. In this diagram the X-axis shows the file size in terms of KB to decrypt and the Y-axis shows the

amount of time required to decrypt. According to the obtained results of the proposed system the performance of the proposed algorithm is much effective.

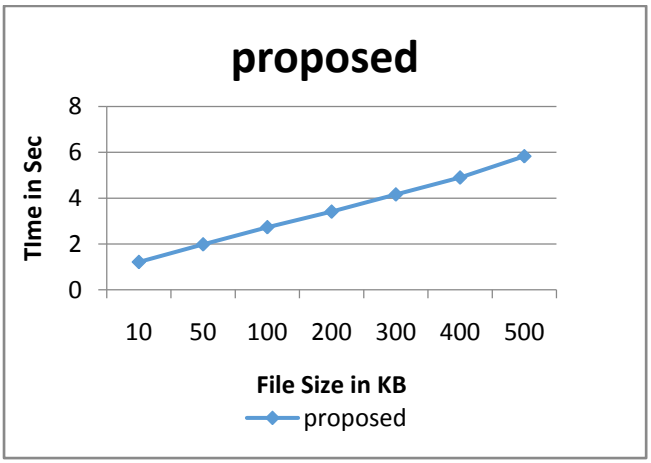

Figure 8 Decryption Time

5.4 Decryption Space Complexity

The amount of main memory required to decrypt the encrypted data is known as the decryption memory consumption or the decryption space complexity. The figure 6 provides the decryption space complexity of the proposed system. To represent the performance of the system X axis contains the amount of file size used for experimentation and the Y axis shows the amount of main memory consumed in terms of KB (kilobytes). According to the obtained results the performance of the proposed technique is found optimum for the decryption space complexity moreover that is rises with the amount of file size increases for decryption.

Figure 9 Decryption Space Complexity

5.5 Mean Square Error Comparison

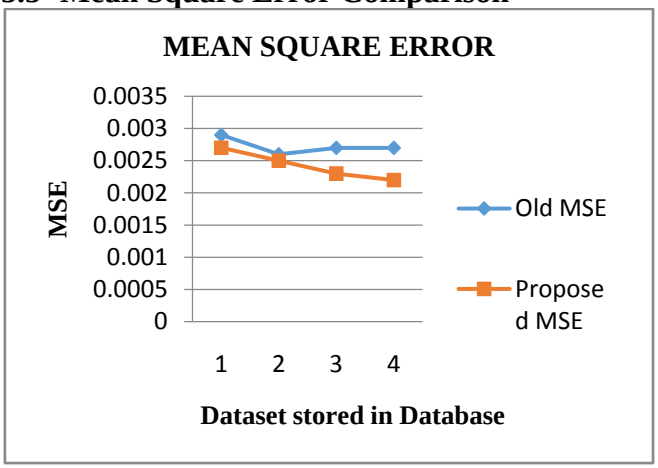

Figure 10 Comparison of MSE

The mean squared error (MSE) of an estimator calculates the average of the squares of the errors or deviations, that is, the difference between the estimator and what is estimated. Figure 7 shows, the graphical representation of MSE values of different data files. The horizontal axis shows the data files and vertical shows the range of MSE value, blue line shows the MSE values of old method [16] whereas red line shows the MSE values of proposed technique. The MSE values for old method are higher than the MSE values of proposed technique as compared in figure 7. Figure 8 shows the Graphical representation of the MSE values of proposed algorithm in implementation.

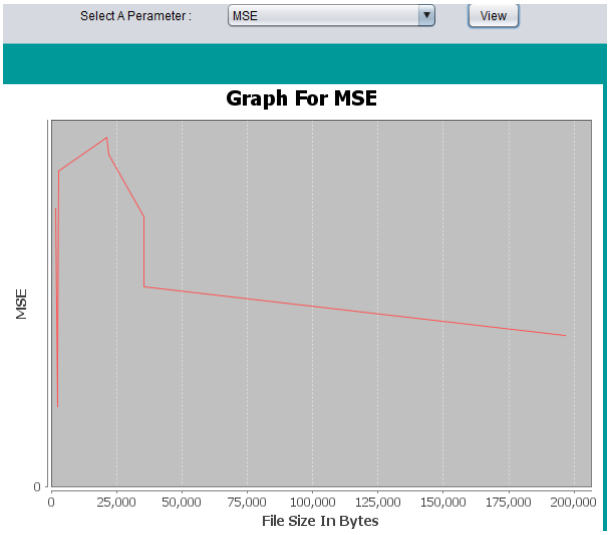

Figure 11 Graphical representation of the MSE values of proposed algorithm in implementation

5.6 Peak Signal to Noise Ratio

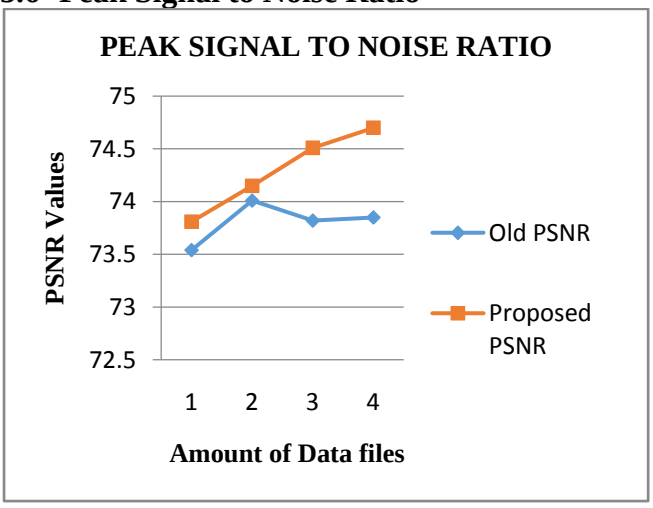

Figure 12 Comparison of PSNR

Peak Signal-to-Noise Ratio is the proportion between the reference signal and the distortion signal in an image, given in decibels [16]. The higher the PSNR, the nearer the distorted image is to the original. In general, a higher PSNR value should correlate to a higher quality image. In Figure 9, the graphical representation of PSNR values of different data files. The horizontal axis shows the data files and vertical shows the range of PSNR value in decibel. Blue line shows the PSNR values of old technique and the red line shows the PSNR values of Proposed Technique. The PSNR values for Old method [16] are lesser than the PSNR values of proposed method as compared in figure. Figure 9 shows the Graphical representation of PSNR values of proposed algorithm in implementation.

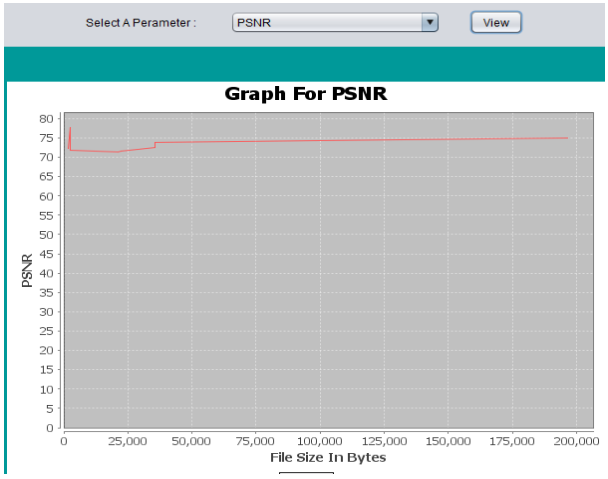

Figure 13 Graphical representation of PSNR values of proposed algorithm in implementation.

6. CONCLUSION

The security is an essential concept of the digital data, it becomes more sensitive when the data is travelled through the untrusted environment. Here the untrusted environment can be any openly accessible network where anybody can use the network facilities. In the presented work, the image based secure steganography is the primary motive to hide the information. Therefore a number of techniques are evaluated and a hybrid technique using the steganography and traditional cryptographic approach is proposed and implemented.

The proposed technique includes the goodness of AES based data cryptography and the LSB based image steganography for hiding the sensitive data on the given cover image. The proposed technique first compress the information to reduce the size of data to be hide, then utilizes the AES cryptographic technique to generate the cipher text. This cipher text is further sub-divided into small fixed size blocks to hide into the image. On the other hand the key image is treated using the genetic process therefore a small modification on traditional genetic algorithm is made to select the rows and low intensity pixels to hide data on LSB of image.

The implementation of the proposed technique is performed using the JAVA technology and their performance in terms of space complexity, time complexity, MSE and PSNR is evaluated. MSE and PSNR and obtained values are much better than existing techniques. The obtained performance of the proposed algorithm is given using table 2.

Table 2 performance summary

S. No.	Parameters	Remark
1	Encryption time	Encryption time in increases with the size of data but needs improvement on the encryption time complexity
2	Decryption time	Decryption time is in similar ratio as the encryption time but need less time as compared to encryption time
3	Encryption memory	The memory consumption of the proposed technique is adoptable and provides efficient outcomes
4	Decryption memory	The decryption memory is also in a regular manner and improved as the file size is increases
5	MSE values	Low
6	PSNR values	High

According to the obtained performance of the proposed technique, the system is adoptable for securing small size data transmission.

7. FUTURE WORK

The proposed work is an effective technique for securing data in unsecured media. But there is a limitation of the system, it efficiently works on the small amount of data. But in near future need to be focused on the development of this algorithm, i.e. to reduce processing time of image encryption to get the efficient output. Apart from this will focus on cipher strength that there are no chances of brute force attack or greatly customize image data to empower security ethics.

8. REFERENCES

[1] Xiliang Liu, "Selective encryption of multimedia content in distribution networks: challenges and new directions", Proceedings of Communications, Internet, and Information Technology (CIIT 2003), Scottsdale, AZ, USA, Nov. 2003.

[2] Falesh M. Shelke et al. "Comparison of different techniques for Steganography in images "International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 2, February 2014.

[3] Pratiksha Sethi and V. Kapoor "A proposed novel architecture for image steganography using Genetic algorithm along with cryptography" ICRTCSE 2016.

[4] M.Kundalakesi, Sharmathi.R and Akshaya.R, "Overview of Modern Cryptography", International Journal of Computer Science and Information Technologies (IJCSIT), Volume 6, PP. 350-353, 2015.

[5] Manoj Kumar Pandey, Mrs. Deepty Dubey, "Survey Paper: Cryptography The art of hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), PP. 3168-3171, Volume 2, December 2013.

[6] Mohammed AbuTaha, Mousa Farajallah and Radwan Tahboub, "Survey Paper: Cryptography Is the Science of Information Security", International Journal of Computer Science and Security (IJCSS), PP. 298- 309, Volume 5, 2011.

[7] Prakash Kuppuswamy, and Saeed Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm", MIS Review: An International Journal, Volume 19, No. 2, PP. 1-13, March 2014.

[8] Priyanka B. Kutade and Parul S. Arora Bhalotra "A Survey on Various Approaches of Image Steganography", International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 3, January 2015

[9] Silman J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[10] Lee Y. K. and Chen L. H., "High capacity image steganographic model", IEEE Proceedings of Visual Image Signal Processing, Vol. 147, No. 3, pp. 288-294, 2000.

[11] Ker A., "Improved detection of LSB steganography in grayscale image", Lecture Notesin Computer Science, pp. 97-115, 2005.

[12] Mahdavi, Samavi Sh., Zaker N. & M Hashemi.,"Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram", Iranian Journal of Electrical & Electronic Engineering, Vol. 4, No. 3, pp. 59-70, 2008.

[13] Manish Trehan and Sumit Mittu, "Steganography and Cryptography Approaches Combined using Medical Digital Images", International Journal of Engineering Research & Technology (IJERT), Volume 4 June 2015.

[14] David E. Goldbrg, "Genetic Algorithm in Search, Optimization & Machine Learning",Pearson Education Asia.

[15] Genetic Algorithms for optimization, Programs for MATLAB Version 1.0 User Manual.

[16] Anil Kumar and Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique" International Journal of Advanced Research in Computer Science and Software Engineering 3(7), July - 2013, pp. 363-372