International Journal of Research in Engineering, Science and Management
Volume-2, Issue-3, March-2019
www.ijresm.com | ISSN (Online): 2581-5792

Secure Text Sharing using Medical Image Steganography

R. Deepika[1], E. Ezhil Arasi[2], M. Geethanjali[3]
[1,2,3]*Student, Department of Biomedical Engineering, DSIT, Trichy, India*

***Abstract*: The increased popularity of digital media has raised serious concerns over its security related issues. Security attacks in the form of eavesdropping, masquerading and in many other forms is very common nowadays. Data hiding is one of the techniques that aim to provide security by hiding secret information into the multimedia contents by altering some nonessential components in the host file. Security of data is important in data communication. A lot of information is transferred from one user to another on internet and it also has the possibility of data theft also increases. Steganography provides a solution for the security during data transmission. Steganography is the science and it makes the valuable information invisible to prevent it from unauthorized user. A steganography system has meet three main requirements namely, imperceptibility of embedding, recovery of embedded information is accurate, and large payload (bits get delivered to the end user at the destination). So in this project an image steganography technique is proposed to hide the documents in image in the transform domain using CMD approach. The document files are carried by the image without revealing the existence to anybody. When the secret information is hidden in the carrier the result is the stego and audio signal. In this work, the results show good quality stego signal with secure key and audio and the stego signal is analyzed for different attacks. The stego signals are transferred to multiple receivers based on network strategies. It is found that the technique is robust and it can withstand from attacks. The quality of the stego image is measured by Peak Signal to Noise Ratio (PSNR) and other measurements.**

***Keywords*: Steganography, Image processing, Data hiding**

1. Introduction

Secure the data is very important in data communication. Steganography provides a solution for the security of information during data transmission as well as secure with voice and key in decryption side. Implement the interface to hide the text in medical images using CMD approach.

A. General

Image processing is a method to convert an image into digital form and do some operations on it, in order to get an enhanced image. It is one of the signal dispensation in which input is image, like video frame and output may be image or characteristics with that image. Now a day it is a growing technology, and its applications in various aspects of a business. Image Processing also form core research area within engineering and computer science field. Image processing systems are becoming popular due to easy availability of powerful personal computer, large sized memory devices and graphics software etc.

Image processing basically includes the following three steps.

- Importing the image by digital photography.
- Analyzing and manipulating the image which includes data compression and image enhancement.
- Output is the last stage in which result can be altered image that is based on image analysis.

Applications of Image processing:

- Remote sensing
- Medical imaging
- Forensic Studies Textiles
- Material science
- Military
- Film industry
- Document Processing

The common steps in image processing are image storing, scanning, enhancing and interpretation. The following Figure 1 shows image processing.

Fig. 1. Image Processing

In the above Figure, an image has been catch by a camera and has been sent to a digital system to remove all the other details, and zooming it to focus on the water drop in such a way that the quality of the image has not changed.

B. Purpose of Image processing

The purpose of Image processing has 5 types,

- *Visualization* - Perceive the objects that are not visible.
- *Image sharpening and restoration* - To produce a better image.
- *Image retrieval* – Look for the image of interest.
- *Measurement of pattern* – Calculate various objects in an image.
- *Image Recognition* – Differentiate the objects in an image.

Types of Image Processing:

The two types of Image Processing are

- Analog image processing
- Digital image processing

C. Analog image processing

Analog or visual techniques of image processing can be majorly used for the hard copies like printouts and photographs. While using these visual techniques, various fundamentals of interpretation are used by Image analyst. The image processing is not confined to area and it has to be studied but on knowledge of analyst. Through visual techniques, an association is another important tool in image processing. So, a combination of personal knowledge and collateral data to image processing can apply by analysts.

D. Digital image Processing

Digital image processing is the computer algorithms to perform image processing on digital images. As a field of digital signal processing, digital image processing has many advantages than analog image processing. It allows wider range of algorithms to be applied to the input data. During processing, problems such as the build-up of noise and signal distortion can be avoided. Since images are explained over two dimensions, digital image processing may be modeled in the form of multidimension.

2. Review of literature

- "Study of efficient compression of encrypted gray scale image" by Wei Lui in 2014.Lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. For encrypted real-world sources like pictures, the key to improve the compression efficiency is how the source dependency is exploited. Approaches within the literature that create use of mathematician properties within the Slepian-Wolf decoder do not work well for grayscale images. In this paper, we propose a resolution, such that the decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. Good performance is observed both theoretically and experimentally. We specialize in the look and analysis of a practical lossless image codec, where the image data undergoes stream-cipher based encryption before compression. We propose resolution progressive compression for this drawback, which has been shown to have much better coding efficiency and less computational complexity than existing approaches. The success of RPC is because of enabling partial access to this supply at the decoder facet to boost the decoder's learning of the supply statistics.
- "Study of Quality Assessment of Color Image Compression using Haar Wavelet Transform" by Sanjeev Kumar in 2011. Images need substantial storage and transmission resources. So compression is advantageous to scale back these necessities. This paper covers some background of rippling analysis, data compression and how wavelets have been and can be used for image compression. The paper examines a group of rippling functions (wavelets)for implementation in an exceedingly still compression system and discusses necessary options of rippling remodel in compression of still pictures, including the extent to that the standard of image is degraded by the method of rippling compression and decompression. The effect of different wavelet functions, image contents and compression ratios are assessed. We have summarized the characteristics of compression, necessity of compression and its principles and EZW and SPIHT image compression algorithms based on rippling. We use 256×256 color image for comparison. Any of the two approaches is satisfactory when the 0.5 bits per pixel (bpp) is requested. However, for a very low bit rate, for example 0.25 bpp or lower, the embedded zero tree wavelet (EZW) approach is superior. Also EZW provides higher compression magnitude relation and quality of pictures. However if for sensible applications, we have a tendency to conclude that (1) rippling primary based compression algorithms are a unit powerfully recommended, (2) DCT primarily based approach may use an adaptive divisional table, (3) VQ approach is not applicable for an occasional bit rate compression even supposing it is simple, (4) Form approach ought to utilize its resolution-free decrypting property for a low bit rate compression.
- "Study of Stream Ciphers Analysis Methods" by Dominic Bucerzan in 2013. The purpose of this paper is to present and to discuss analysis methods applied in symmetric cryptography, especially on stream ciphers. The tests were created on algorithmic programs and additionally on the non-public parallel cryptanalytic algorithm, HENKOS, based on a pseudorandom number generator. The check confirms that the algorithmic programs seems to be secure and quick. The paper describes initial, the most components of the cryptosystem, its implementation and different analysis methods. The code is written in the C/C++ language. The package application and therefore the tests applied were processed on a laptop, PC. The quality analysis presents the results of the many applied math tests, comparing some algorithms based especially on pseudo random number generators. The tests use normal sequence of 12.5 MB resulted from some test generators. The main part of the work presents hand-picked results for the foremost vital applied math tests like: FIPS 1401, FIPS 1402, ENT tests, Diehard battery of tests, NIST Statistical

Test Suite. There are a lot of stream ciphers used in cryptography because of the speed, but in this case nobody tried standardization like in block cipher area. The European Union–based Nessie project, was aimed at evaluating the security of various cryptanalytic primitives, did not recommend any stream ciphers in their report. The performances and quality analysis on cryptanalytic stream ciphers algorithms are a bold goal for all the designers of algorithms. In majority of cases there's no proof of the behaviour of the new cipher, but it's possible to verify the quality by performing statistical tests, and also to measure the performances of implementation and therefore the speed by package means that. There is a great deal of stream ciphers utilized in cryptography owing to the speed, however during this case no one tried a standardization like in block cipher space. In the future, new stream ciphers will appear so that new methods for analysis will be permanent preoccupation for the cryptographic community.

- "Study of Robust Embedded Data from Wavelet Coefficient" proposed by J.J.Chae in 2004. An approach to embedding Grey scale pictures employing a distinct wave remodel is projected. The projected theme allows mistreatment signature pictures that might be the maximum amount 25% of the host image knowledge and hence may well be used each in digital watermarking as well as image/data hiding. In digital watermarking the first concern is that the recovery or checking for signature even once the embedded image has been modified by image process operations. Thus the embedding theme ought to be study to typical operations like low-pass filtering and lossy compression. In distinct, for data hiding applications it is important that there should not be any visible changes to the host data that is used to transmit a hidden image. In addition, in both knowledge concealing and watermarking, it is desirable that it is difficult or impossible for unauthorized persons to recover the embedded signatures. The projected theme provides a straightforward management parameter that may be tailored to either concealment or watermarking functions, and is robust to operations such as JPEG compression. Experimental results demonstrate that prime quality recovery of the signature knowledge is feasible. A scheme for image embedding is presented. This approach may be used for each digital watermarking connected applications furthermore as for data hiding purposes. The scale factor controls the relative amount of host and signature image data in the embedded image. A larger multiplier may be used for data hiding wherever it's fascinating to keep up the sensory activity quality of the embedded image. A lower multiplier is best suited to watermarking wherever hardiness to typical image processing operations is required. Experimental results demonstrate that good quality signature recovery and authentication is possible when the images are quantized and JPEG compressed by as much as 90%. In digital watermarking, the signatures are sometimes of abundant smaller dimensions (in terms of range of bytes needed) compared to the host image. Since the projected technique will manage a considerably larger range of signature knowledge, it is possible to distribute the signature spatially as well, thus making watermarking robust to operations such as image cropping. Even though the Haar wave basis is employed in the experiments, the method can be easily adopted to other wavelet transforms and for more than one level of decomposition. It might be worth exploring the utilization of different basis functions counting on the characteristics of the host and signature pictures.
- "Study of Spatial Domain Image Steganography Technique" by B.Sunitha Devi in 2012. Steganography is that the art and science of concealing information by embedding information into cowl media. In this paper we tend to propose a brand new methodology of information concealing in digital image in spatial domain. In this method we use Plane Bit Substitution Method (PBSM) technique in which message bits are embedded into the pixel value(s) of an image. We first, projected a Steganography transformation machine (STM) for determination operation for manipulation of original image with facilitate to least significant bit (LSB) operator primarily based matching. Second, we tend to use pixel encoding and decoding techniques below theoretical and experimental evolution. Our experimental, techniques are sufficient to discriminate analysis of stego and cover image as each pixel based PBSM, and operand with LSB. The security and the size of stored data, a new adaptive LSB technique is used. Instead of storing the data in every least significant bit of the pixels, this technique tries to use more than one bit in a pixel in such a way that this alteration won't have an effect on the visual look of the host image. It uses the side information of neighbouring pixels to estimate the number of bit which can be carried in the pixels of the host-image to hide the secret data called PBSM. To increase the security and the size of stored data, a new adaptive LSB technique is used. Instead of storing the data in every least significant bit of the pixels, this technique tries to use more than one bit in a pixel in such a way that this change will not affect the visual appearance of the host pictures.
- "Study of Content Adaptive Steganography" by Voj-

tech holub. The goal of steganography is to speak secret messages while not revealing the terribly existence of the key communication. This can be achieved by hiding the messages in inconspicuous objects. The focus of this dissertation is on steganography by cover modification, where the covers are ray scale digital images in either spatial or JPEG domain. Grayscale images are used for simplification as the majority of the principles can be extended to colour images as well. Other known types of steganography are steganography by cover selection and by cover synthesis Due to high complexity of support vector machines for supervised classification, the machine learning of choice in this dissertation is the ensemble classifier. For problems in steganalyzer with a large number of very weak features and cover-steno training pairs in the training set, it offers a comparable performance for a fraction of the computational costs when compared with support vector machines. The significantly lower training complexity allows the steganalyst to design high dimensional statistical features and train on larger training sets, consequently greatly improving detection of modern steganographic schemes. This section provides explanation of ensemble's basic principles. There are two ways of designing good steganographic algorithms for digital images. The first method relies on a defined cover image model, which is preserved by steganography. The second and modern approach is steganography by minimizing some, usually heuristically defined, embedding distortion function.

3. Methodology

A. Block diagram

The proposed system is designed to provide solution for the drawback of existing system. The block diagram for proposed system is shown in Fig. 2. The description of each block is explained below.

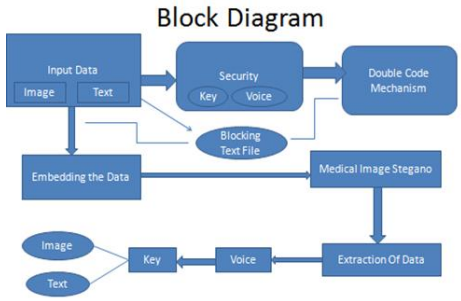

Fig. 2. Block diagram

B. Conventional process

Computer rhetorical (sometimes called as computer forensic science) may be a branch of science relating legal proof found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions about the information. Although it is most frequently related to the investigation of large style of computer crime, computer forensics may be employed in civil proceedings. The discipline involves similar techniques and principles to information recovery, however with further pointers and practices designed to create a legal audit path. Computer rhetorical is that the appliance of examination and analysis techniques to collect and preserve proof from choosing computer in an exceedingly means is acceptable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation whereas maintaining a documented chain of proof to search out specifically what happened on a computer and who was responsible for it. Forensic investigators usually follow a regular set of procedures: When physically analytic the device in question to create positive it cannot be accidentally contaminated; investigators build a digital copy of the device's storage media. Once the first media has been derived, it is barred in a very safe or alternative secure facility to keep up its pristine condition. All investigation is done on the digital copy. Investigators use a range of techniques and proprietary software system rhetorical applications to look at the copy, looking hidden folders and unallocated disc space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation. Computer rhetorical has become its own space of scientific experience, with incidental work and certification. A secure method of data hiding will be used in the project which provides authentication, data integrity and confidentiality with audio. The combination of encryption and data hiding can solve these types of problems by using reversible data hiding method for images. It will be able to embed data in images. The main goal of steganography is to speak firmly in a very utterly undetectable manner and to avoid drawing suspicion to the transmission of a hidden information. It is not to keep others from knowing the hidden data, but it is to keep others from thinking that the information even exists. If a steganographic method causes someone to suspect the carrier medium, then the method has failed. In proposed system we can implement clustering modification direction strategies to embed the text into images with audio. This technique is known as spatial domain techniques which use the pixel gray levels and their color values directly for encoding the message bits. These techniques are a unit a number of the only schemes in terms of embedding and extraction complexness. And implement password with audio protection approach to encode the data. The encoded data embedded into images as stego image. Finally extract test and images based inverse operations. We can hide the data as in the

type of files and shared to multiple users based on local area connection. The embedded image can be transfer to receiver in secure manner and the extraction of data with audio secure can't be lost and measured by quality parameters.

C. Implementation

The amount of digital pictures has accumulated apace on the Internet. Image security becomes progressively necessary for several applications, e.g., confidential transmission, video police investigation, military and medical applications. For example, the need of quick and secure identification is important within the medical world. Nowadays, the transmission of pictures could be a daily routine associate degree and it is necessary to seek out an economical thanks to transmit them over networks. To decrease the data loss, we need data hiding algorithms. Since few years, a problem is to try to combine data hiding and clustering in a single step. So we can implement clustering mechanisms to choose the pixel location and provide password details to protect the data from hacking.

Modules:

- Image and data acquisition
- Pixel conversion
- Embedding the data with audio
- Extraction of the data with audio
- Evaluation criteria

Modules description:

Image and data acquisition:

Steganography is an art of hiding some secret message in another message without letting anyone know about presence of secret message except the intended receiver. The file is used to hide secret file is called host file or cover file. Once the contents of the host file or cover file are modified, the resultant message is known as stego message. In this module, user can upload the cover image and data which is hiding in cover image. Then read the image as pixel format and data as text format. We can upload any length of text.

D. Pixel conversion

Cover image is represented in color channel. Then using clustering modification transformation approach which is a decomposition of a function into a linear combination of the spatial features. Then extract clip image from uploaded images. In this module, consider the embedded data file upload the image. The noise uses the data hide message. Pixel into pixel divides the image. Use the layer embedded the code for override of the image. The file uploads the image use the stegnoanalyzer data hide for the result. So that modifications of same direction. The overall distortion because the costs of dynamically updated. The total number of pixel value of ratio and modified pixels. Here the direction the choice of positively or negatively changing the intensity of pixel.

E. Embedding the data with audio:

In this module, select the approximation and detailed co-efficient values. Then hide the data in approximation coefficients in second plane. Then provide password to protect the input data. In this model we will use the password based algorithm, which will convert the text, which provide a high security. And this data is stored in images after that image can be send with audio. At the receiving side, the shares are retrieved and converted to original image by stacking them together. After that implement inverse approach to get stego image with audio. Stego image is then converted in RGB format.

F. Extraction of data

In this module, original image and data is extracted with improved manner. We can read the stego image and convert it into RGB format and get the inverse sub bands from stego image. Then decode the stego image to get the text in encrypted format with audio. Apply decryption to get original data. We can get the binary values of text to convert into the decimal values. Finally using inverse transform to extract cover image and data.

G. Evaluation criteria

In this module we evaluate the performance by using PSNR and SSIM measure, PSNR is employed to evaluate the quality of marked decrypted image quantitatively. SSIM in this project is used for distinguishing between natural and pseudo boundary pixels and its size is critical to practical applicability of proposed approach.

H. Digital image Processing

Digital image processing is that the use of pc algorithms to perform image processing on digital pictures. As a subcategory or field of digital signal process, digital image process has several blessings over analog image process. It permits a way wider vary of algorithms to be applied to the computer file and might avoid issues like the build-up of noise and signal distortion throughout process. Since pictures square measure outlined over 2 dimensions (perhaps more) digital image process could also be sculptural within the variety of two dimensional systems. Many of the techniques of digital image process, or digital picture process because it usually was referred to as, were developed in the 1960. The cost of process was fairly high, however, with the computing instrumentation of that era. That modified within the seventies, once digital image process proliferated as cheaper computers and dedicated hardware became available. Images then can be processed in real time, for a few dedicated issues like television standards conversion. As all-purpose computers became quicker, they began to take over the role of dedicated hardware for nearly the foremost specialized and computer-intensive operations. With the quick computers and signal processors offered within the 2000s, digital image process has become the foremost common variety of image processing and usually, is used because it is not solely the foremost versatile methodology, however additionally the most affordable. Digital Process techniques facilitate in manipulation of the digital pictures by exploiting

computers. As raw data from imaging sensors from satellite platform contains deficiencies. To get over such flaws and to induce originality of knowledge, it is to bear varied phases of process. The three general phases that each one kind of knowledge have to be compelled to bear whereas exploitation digital technique are Pre- processing, improvement and show, information extraction.

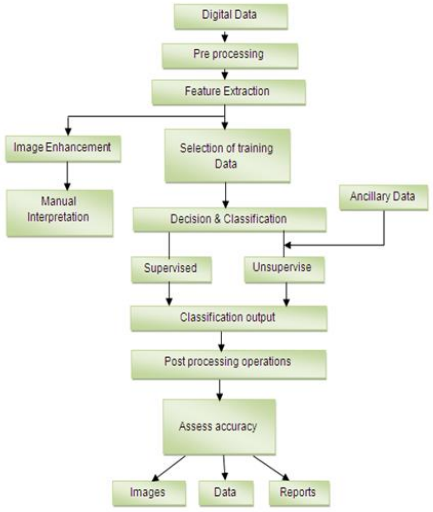

Fig. 3. Block diagram of digital image processing

The various image enhancements and image processing techniques

- Enhancement
- Convolution
- Math processes
- Noise filters
- Trend removal
- Edge detection
- Image analysis
- Image segmentation
- Image recognition

I. Enhancement

Enhancement programs make information more visible.

- Histogram equalization-Redistributes the intensities of the image of the entire range of possible intensities (usually 256 gray-scale levels).
- Unsharp masking-Subtracts smoothed image from the original image to emphasize intensity changes.

J. Convolution

Convolution programs square measure 3-by-3 operative on constituent neighborhoods.

- Highpass filter-Emphasizes regions with rapid intensity changes.
- Lowpass filter-Smoothes images, blurs regions with rapid changes.

K. Math processes

Math processes programs perform a variety of functions.

- Add images-Adds two images together, pixel-by-pixel.
- Subtract images-Subtracts second image from first image, pixel by pixel.
- Exponential or logarithm-Raises e to power of pixel intensity or takes log of pixel intensity.
- Scalar add, subtract, multiply, or divide-Applies the same constant values as specified by the user to all pixels, one at a time. Scales pixel intensities uniformly or non-uniformly
- Dilation-Morphological operation expanding bright regions of image.
- Erosion-Morphological operation shrinking bright regions of image.

L. Noise filters

Noise filters decrease noise by diminishing statistical deviations.

- Adaptive smoothing filter-Sets pixel intensity to a value somewhere between original value and mean value corrected by degree of noisiness. Good for decreasing statistical, especially single-dependent noise.
- Median filter-Sets pixel intensity equal to median intensity of pixels in neighborhood. An excellent filter for eliminating intensity spikes.
- Sigma filter-Sets pixel intensity equal to mean of intensities in neighborhood within two of the mean. Good filter for signal-independent noise.

M. Trend removal

Trend removal programs take away intensity trends varying slowly over the image.

- Row-column fit-Fits image intensity along a row or column by a polynomial and subtract fit from data. Chooses row or column in step with direction that has the smallest abrupt changes.

N. Edge detection

Edge detection programs sharpen intensity-transition regions.

- First difference-Subtracts intensities of adjacent pixels. Emphasizes noise as well as desired changes.
- Sobel operator-3-by-3 mask weighs inner pixels twice as heavily as corner values. Calculates intensity differences.

O. Image analysis

Image analysis programs extract information from an image.

- *Gray-scale mapping*-Alters mapping of intensity of pixels in file to intensity displayed on a computer screen.
- *Slice*-Plots intensity versus position for horizontal, vertical, or arbitrary direction. Lists intensity versus constituent location from any purpose on the slice.

- *Image extraction:* Extracts a portion or all of an image and creates a new image with the selected area.
- *Images statistics:* Calculates the maximum, minimum, average, standard deviation, variance, median, and mean-square intensities of the image data.

P. Image segmentation

Image segmentation is that the strategy of separating a digital image into multiple segments (sets of pixels, also conjointly called super pixels. Image segmentation is usually wont to find objects and limits (lines, curves, etc.) in images. More exactly, image segmentation is that the method of distribution a label to each picture element in a picture specified pixels with constant label share bound characteristics. The result may be image segmentation is a set of segments that together cowl the complete image, or a set of contours extracted from the image (see edge detection). Each of the pixels during a region square means are similar with relation to some characteristic or computed property, such as color, intensity, or texture. Adjacent regions square measure is considerably completely different with relation to the similar characteristic.

Image segmentation is the process of separating a digital image into multiple segments.

- The aim of segmentation is to modify or change the characterization of the picture into something that is more meaningful and easier to analyze. Image segmentation is usually wont to find objects and limits in pictures.
- Image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain characteristics.

4. Testing &Result

A. Testing

A test case is an asset of data that the system will process as normal input. The strategies that we have used in our project are,

1) System Testing

Testing is the stage of implementation of which aimed at ensuring that the system works accurately and efficiently before live operation commences. Testing is important to the success of the system. System testing makes a logical assumption that if all the components of the system are correct the goal will be achieved. The candidate's system subject to a range of tests. Online response, stress, recovery, security and usability tests. A series of testing are performed for the planned system before the system is prepared for user acceptance testing.

2) Unit testing

The procedure level testing is made first. By giving improper inputs, the errors occurred are noted and eliminated. Then the web form level is made.

3) Integration Testing

Testing is done for each module. After testing all the modules, the modules are integrated and testing of the system is done with the test data, specially designed to show that the system will operate successfully in all its aspects conditions. Thus the system testing could be confirmation that each one its correct and a chance to point out the user that the system works.

4) Validation testing

The final step involves validation testing that determines whether or not the software package perform because the user expected. The end-user instead of the system developer conduct this check most software package developers as the method referred to as "Alpha and Beta test" to uncover that solely the end user appears able to find. The compilation of the whole project is based on the complete satisfaction of the tip users.

5) Acceptance Testing

Acceptance testing can be defined in many ways, but a simple definition is the succeeds when the software functions in a manner that can be reasonable expected by the customer. After the acceptance check has been conducted, one of the two possible conditions exists. This is to fine whether or not the inputs square means accepted by the information or alternative validations. For example, accept only numbers in the numeric field, date format data in the date field. Also the null check for the not null fields. If any error occurs then show the error messages.

- The function of performance characteristics to specification and is accepted.
- A deviation from specification is uncovered and a deficiency list is made.

5. Results

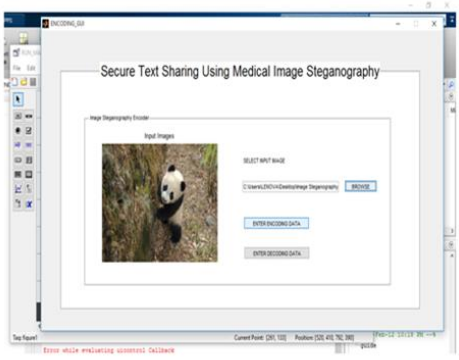

Fig. 4. Diagram of Input Image

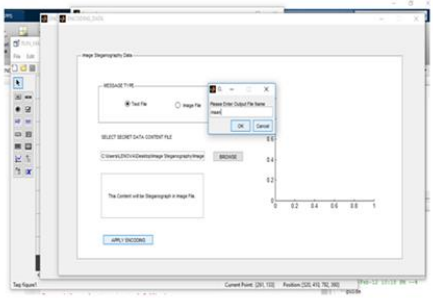

Fig. 5. Diagram of Encoding

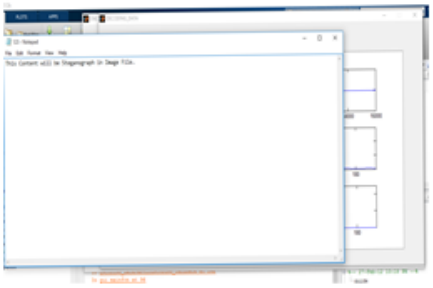

Fig. 6. Diagram of output image

6. Conclusion

The information concealing is that the principle of segregation of the planning choices in a very computer virus that are possibly to alter, thus protecting other parts of the program from in depth modification if the look call is modified. The protection involves providing a stable interface that protects the rest of the program from the implementation (the details that square means that presumably to change). We conclude that hide the data in images for privacy preserving requirements. Our proposed systems use the clustering modification strategies approach to embed data in image. The proposed method can take advantage of all traditional data hiding techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve less payload, separate data extraction and greatly improvement on the quality of marked stego images

References

[1] J. J. Chae and B. S. Manjunath, “A Robust Embedded Data from Wavelet Coefficients,” University of California, Santa Barbara, Ca 93106
[2] Yun Q. Shi, “Reversible Data Hiding,” New Jersey Institute of Technology, Newark, Nj 07102, USA.
[3] Kamrul Hasan Talukder and Koichi Harada, “Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image,”
[4] Musbah J. Aqel, Ziad A. Alqadi, Ibraheim M. El Emary, “Analysis of Stream Cipher Security Algorithm,” Journal of Information and Computing Science, Vol. 2, No. 4, 2007, Pp. 288-298.
[5] S.Imaculate Rosaline, C. Rengarajaswamy, “A Steganographic Substitution Technique Using Appm For Encrypted Pixels,”.
[6] Sapna Sasidharan and Deepu Sleeba Philip, “A Fast Partial Image Encryption Scheme with Wavelet Transform and Rc4,” International Journal of Advances in Engineering & Technology.
[7] Manikandan R, Uma M, “Reversible Data Hiding for Encrypted Image,” Journal of Computer Applications, Vol. 5, February 2012.
[8] C. Rengarajaswamy and K. Vel Murugan, "Separable extraction of concealed data and compressed image," *2013 International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT)*, Tiruvannamalai, 2013, pp. 1-5.
[9] P. Tsai, Y. C. Hu, And H. L. Yeh, “Reversible Image Hiding Scheme Using Predictive Coding and Histogram Shifting,” Signal Process., Vol. 89, pp. 1129–1143, 2009.
[10] L. Luo Et Al., “Reversible Image Watermarking Using Interpolation Technique,” IEEE Trans. Inf. Forensics Security, Vol. 5, No. 1, pp. 187–193, Mar. 2010.