ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 2, April 2017

Secure Data Transmission Using Clustering Modification Direction

Mrs.N.Vaijayanthi M.E,(Ph.D.)
Head of the Department
Department of Electronics Communication Engineering
Indra Ganesan College of Engineering
Trichy-12, Tamil Nadu, India

K. MADHUBALA, J.SARANYADEVI,
N.SOWNDHARYA, S.VALARMATHI.
Department of Electronics Communication Engineering
Indra Ganesan College of Engineering
Trichy-12, Tamil Nadu, 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 tampering and in many other forms is very common nowadays. Data hiding is one of the emerging techniques that aim to provide for security by hiding secret information into the multimedia contents by altering some nonessential components in the host or cover file. Security of data is very important in data communication. Everyday a lot of information is transferred from one user to another on internet and so the possibility of data theft also increases. Steganography provides a solution for the security of information during data transmission. Steganography is the science which makes the valuable information invisible to prevent it from unauthorized user. A steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding, accurate recovery of embedded information, and large payload (payload is the bits that get delivered to the end user at the destination). So in this project an image steganography technique is proposed to hide text signal in image in the transform domain using ECC approach. The text signal in any format is encrypted and carried by the image without revealing the existence to anybody. When the secret information is hidden in the carrier the result is the stego signal. In this work, the results show good quality stego signal and the stego signal is analyzed for different attacks. It is found that the technique is robust and it can withstand the attacks. The quality of the stego image is measured by Peak Signal to Noise Ratio (PSNR), and other measurements.**

Keywords—Elliptic curve Crypotography, Information hiding, Encrypted image, Clustering Modifiation Direction.

1. INTRODUCTION

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It is a type of signal dispensation in which input is image, like video frame or photograph and output may be image or characteristics associated with that image. Usually Image Processing system includes treating images as two dimensional signals while applying already set signal processing methods to them. It is among rapidly growing technologies today, with its applications in various aspects of a business. Image Processing forms core research area within engineering and computer science disciplines too. Image processing systems are becoming popular due to easy availability of powerful personal computer, large size memory devices, graphics software etc.

1.1. IMAGE PROCESSING BASICALLY INCLUDES THE FOLLOWING THREE STEPS

- Importing the image with optical scanner or by digital photography.
- Analyzing and manipulating the image which includes data compression and image enhancement and spotting patterns that are not to human eyes like satellite photographs.
- Output is the last stage in which result can be altered image or report that is based on image analysis.

1.2. PURPOSE OF IMAGE PROCESSING

The purpose of Image processing has 5 types,

- Visualization - Observe the objects that are not visible.
- Image sharpening and restoration - To create a better image.
- Image retrieval - Seek for the image of interest.
- Measurement of pattern – Measures various objects in an image.
- Image Recognition – Distinguish the objects in an image.

2. TYPES OF IMAGE PROCESSING:

The two types of Image Processing are

1. Analog image processing
2. Digital image processing

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 2, April 2017

2.1. ANALOG IMAGE PROCESSING:

Analog or visual techniques of image processing can be used for the hard copies like printouts and photographs. Image analysts use various fundamentals of interpretation while using these visual techniques. The image processing is not just confined to area that has to be studied but on knowledge of analyst. Association is another important tool in image processing through visual techniques. So analysts apply a combination of personal knowledge and collateral data to image processing.

2.2. DIGITAL IMAGE PROCESSING:

Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems.

Many of the techniques of digital image processing, or digital picture processing as it often was called, were developed in the 1960. The cost of processing was fairly high, however, with the computing equipment of that era. That changed in the 1970s, when digital image processing proliferated as cheaper computers and dedicated hardware became available. Images then could be processed in real time, for some dedicated problems such as television standards conversion. As general-purpose computers became faster, they started to take over the role of dedicated hardware for all but the most specialized and computer-intensive operations.

With the fast computers and signal processors available in the 2000s, digital image processing has become the most common form of image processing and generally, is used because it is not only the most versatile method, but also the cheapest.

Digital Processing techniques help in manipulation of the digital images by using computers. As raw data from imaging sensors from satellite platform contains deficiencies. To get over such flaws and to get originality of information, it has to undergo various phases of processing. The three general phases that all types of data have to undergo while using digital technique are Pre- processing, enhancement and display, information extraction.

3. THE VARIOUS IMAGE PROCESSING TECHNIQUES

3.1.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.

3.2.Convolution

Convolution programs are 3-by-3 masks operating on pixel neighborhoods.

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

3.3.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. Nonlinearly accentuates or diminishes intensity variation over the image.
- 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.

3.4. 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.

3.5.Trend removal

Trend removal programs remove 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 according to direction that has the least abrupt changes.

3.6.Edge detection

Edge detection programs sharpen intensity-transition regions.First difference-Subtracts intensities of adjacent

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 2, April 2017

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.

3.7.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 pixel location from any point along 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.

3.8. Image segmentation

Image segmentation is the process of partitioning a digital image into multiple segments (sets of pixels, also known as super pixels). The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to locate objects and boundaries (lines, curves, etc.) in images. More precisely, 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.

The result of image segmentation is a set of segments that collectively cover the entire image, or a set of contours extracted from the image (see edge detection). Each of the pixels in a region are similar with respect to some characteristic or computed property, such as color, intensity, or texture. Adjacent regions are significantly different with respect to the same characteristic.

- Image segmentation is the process of partitioning a digital image into multiple segments.
- The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to locate objects and boundaries in image.
- 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. BASIC COLORS

4.1. RGB:

The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. The name of the model comes from the initials of the three additive primary colors, red, green, and blue. The main purpose of the RGB color model is for the sensing, representation, and display of images in electronic systems, such as televisions and computers, though it has also been used in conventional photography. Before the electronic age, the RGB color model already had a solid theory behind it, based in human perception of colors.RGB is a device-dependent color model: different devices detect or reproduce a given RGB value differently.

4.2. CMYK:

The CMYK color model (process color, four color) is a subtractive color model, used in color printing, and is also used to describe the printing process itself. CMYK refers to the four inks used in some color printing: cyan, magenta, yellow, and key (black). Though it varies by print house, press operator, press manufacturer, and press run, ink is typically applied in the order of the abbreviation. The "K" in CMYK stands for key because in four-color printing, cyan, magenta, and yellow printing plates are carefully keyed, or aligned, with the key of the black key plate. Some sources suggest that the "K" in CMYK comes from the last letter in "black" and were chosen because B already means blue However, this explanation, although useful as a mnemonic, is incorrect. The CMYK model works by partially or entirely masking colors on a lighter, usually white, background. The ink reduces the light that would otherwise be reflected. Such a model is called subtractive because inks "subtract" brightness from white.

5. ABOUT THE PROJECT

The main aim of steganography is to increase the steganographic capacity and enhance the imperceptibility while maintaining the robustness.

5.1.Capacity: Capacity is the maximum amount of secret information that can be embedded in a file. Capacity either can be defined as an absolute value in term of number of bits for particular cover or as a relative number regarding necessary bits to save final stego file. Capacity value depends on both embedding function and cover properties (x (0)).

5.2. Imperceptibility: A steganographic system is perfectly secure if the statistics of the cover file and that of the stego file are identical. The higher fidelity of stego object, will give the better imperceptibility. This property would be satisfied if difference of resultant stego file be not distinguishable from original cover. Peak Signal to Noise Ratio (PSNR) is a metric to evaluate the ratio between possible maximum signal and influence of modifying noise to fidelity of its representation. The goal of the stego system is to achieve high PSNR value inorder to make steganography successful.

5.3.Robustness: Robustness is property of harness of eliminating secret information from stego file. While detection of embedded secret data has much higher importance than its

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 2, April 2017

removal, but property of robustness talks about resisting against intentional distortion of communication channel by means of systematic interface or channel noise aiming to ban use of steganography techniques. Robustness metrics of steganographic algorithms are classified in distortion classes like geometric transformations or additive.

6. PROPOSED SYSTEM

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, 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. 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 some of the simplest schemes in terms of embedding and extraction complexity. And implement lifting wavelet approach to choose the approximation and detailed co-efficient values based on lifting scheme. Then encode the text using XOR operation. The encoded text embedded into images as stego image. Finally extract text and images based inverse operations.

6.1. Advantages

1. Noise ratios are reduced.
2. Structures can't be corrupted at extraction phase.
3. Payload can be reduced.
4. Image and text can be extracted successfully without any loss.

6.2 Block Diagram

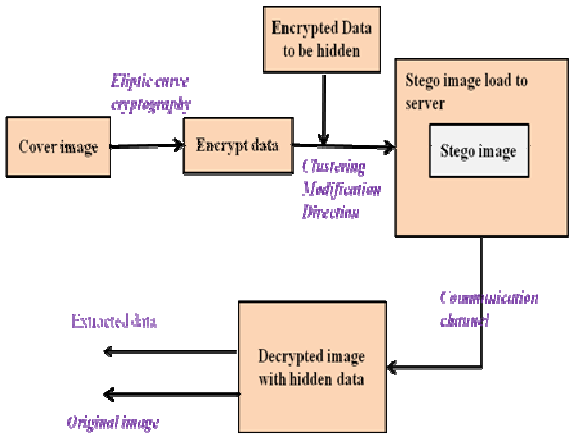

Fig. 1 Framework of the Proposed Method

The proliferation of the Internet has made it possible for anybody to send and receive information instantly from anywhere around the world. Communication of secret information is a major challenge and its complexity increases with the levels of sophistication. Steganography is a form of data hiding technique that provides mechanism for securing data over insecure channel by concealing information within information. It is based on invisible communication and this technique strives to hide the very existence of the secret message from the observer. As a result it is very commonly used by Intelligence Agencies for securely broadcasting and communicating information over the internet by hiding secret information inside images and text. Imperceptibility, robustness and capacity of the hidden data are the main characteristics of steganography.

- The admin get the image and text from database
- Perform wavelet transformation approach to provide pixel and text bands
- Embed text and image, then stored as stego image
- Extract the image and text using inverse wavelet approach with any quality loss.

7. SYSTEM IMPLEMENTATION

Modules description

7.1Image and text 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 message used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stego message. In this module, user can upload the cover image and text which is hiding in cover image. Then read the image as pixel format and text as signal format. We can upload any type of images and text.

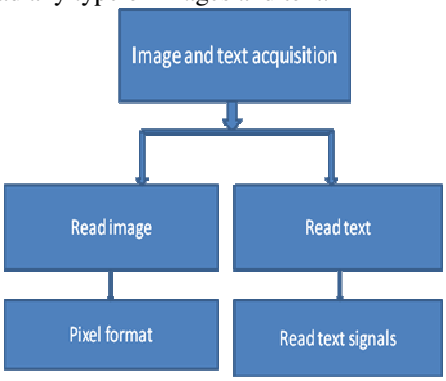

Fig.2 Image and Text Acquisition

7.2. Pixel Conversion:

Cover image is represented in YCbCr channel. Then using clustering modification transformation approach which is a decomposition of a function into a linear combination of the spatial features. The inverse wavelet transform shows that the original signal may be synthesized by summing up all the projections of the signal onto the spatial basis. In this sense, the continuous transform behaves like an orthogonal

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 2, April 2017

transform. Lifted wavelet transform approach which uses integer to integer transformation which is implemented using lifting wavelet transformation (LWT). LWT uses Lifting Scheme (LS). In LS, among the various wavelets available, appropriate wavelet is chosen. As integer coefficients are required, 'int2int' transformation has to be specified. Based on the LS, apply the LWT to cover text to get detail and approximation coefficients, CD and CA respectively. Convert CD to binary. And also do the same process in text signals.

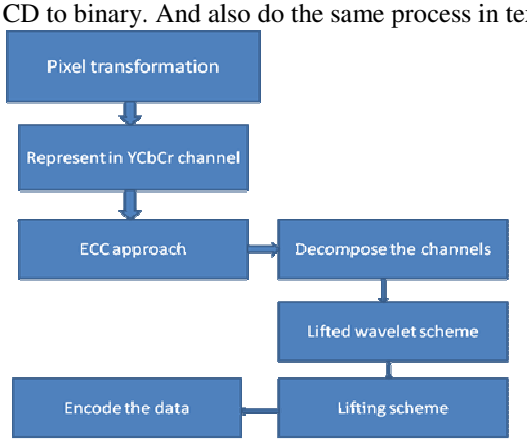

Fig.3 Pixel Transformation

7.3. Embedding the Data:

In this module, select the approximation and detailed co-efficient values. Then hide the text in approximation coefficients in second plane. This process is known as text encryption. In this model we will use the XOR 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. 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. Stego image is then converted in RGB format.

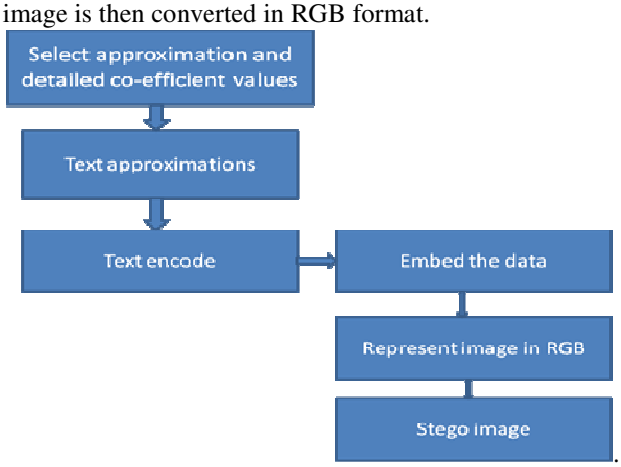

Fig.4 Embedding the Data

7.4. Extraction of Data

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

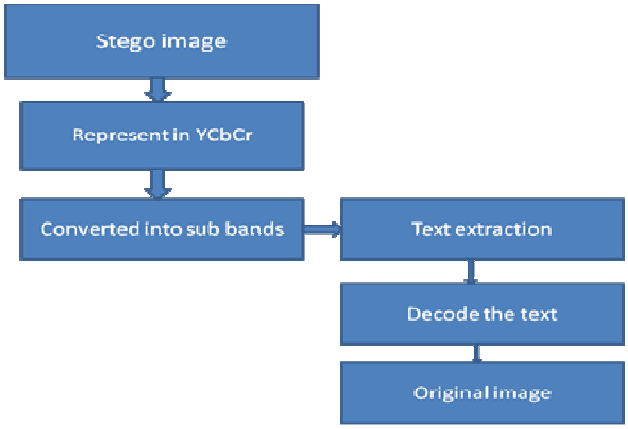

Fig.5 Extraction of Data

7.5.Evaluation criteria

In this module, we evaluate the performance of the system using Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), Universal Image Quality Index (UIQI). The quality of extracted secret text signal is measured by Signal to Noise Ratio (SNR), Squared Pearson Correlation Coefficient (SPCC).

8. EXPERIMENTAL RESULTS

The following image which has been used to the steganographic approach. 'Lena', 'Airplane', 'Barbara'. The steganographic approach is applied to the image.Then study is performed to show the efficiency and performance.In the experimental result,comparison analysis of the EXISTING and PROPOSED SYSTEM is provided.The image of type .jpg is taken to the process.For the algorithm used in the existed system the embedding rate and the PSNR value is low.In the proposed system the ECC algorithm can be used for the encryption and CMD method can be used for hiding the data.The experimental results of the EXISTING algorithm which is given below on comparing with the PROPOSED algorithm which gives efficient result.The comparison of embedding rate value and its percentage improvement can be provided.The following provides the comparative analysis of two methods.

TABULATION:

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 2, April 2017

Table.1 Comparison of the Maximal Embedding Rate (bpp)

Method	Lena	Airplane	Barbara
Existing[8]	37.6	44.5	43.2
Proposed	44.9	51.2	52.8

Table.2 Comparison of Percentage Improvement for Embedding Rate.

Table.3 Comparison of PSNR(db)

Method	Lena	Airplane	Barbara
Existing[7]	0.033	0.05	0.027
Existing [8]	0.043	0.064	0.03
Proposed	0.127	0.096	0.052

9. GRAPH ANALYSIS

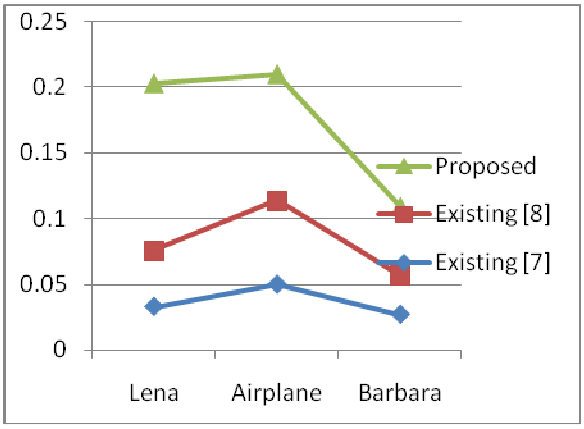

Fig.6 Graph Between EMBEDDING RATE (bpp) of Proposed and Existing

Method	Lena	Airplane	Barbara
Existing[8]	33.3	28	11.1
Proposed	97.5	75	86.2

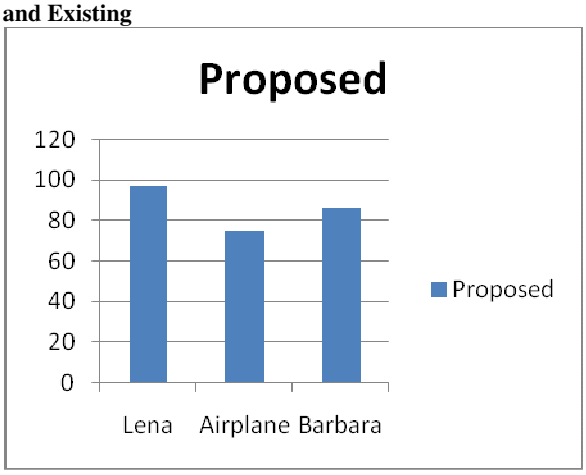

Fig.7 Column Chart for PERCENTAGE IMPROVEMENT in Proposed system

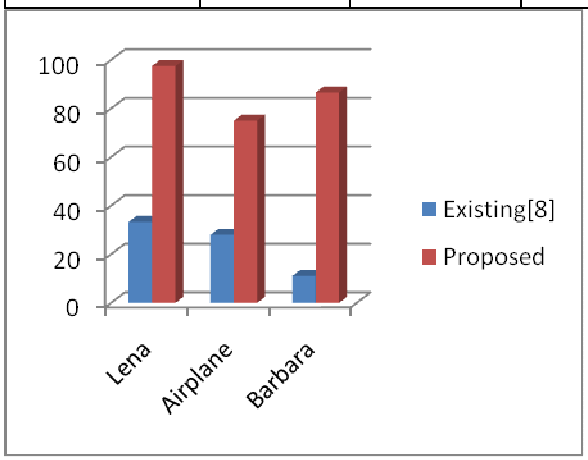

Fig.8 Column chart of PERCENTAGE IMPROVEMENT for Proposed and Existing system

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 2, April 2017

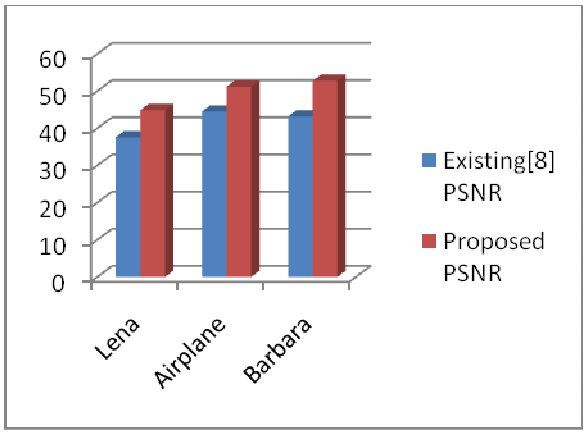

Fig.9 Column chart of PSNR (db) for Proposed and Existing System

10. CONCLUSIONS

The information hiding is the principle of segregation of the design decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed. The protection involves providing a stable interface which protects the remainder of the program from the implementation (the details that are most likely to change). We concludes that hide the text in images for privacy preserving requirements. Our proposed systems use the clustering modification strategies approach to embed text 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

11. FUTURE ENHANCEMENT

In future work, we can extend our project in video domain to provide an efficient and a secure method for video steganography. The proposed method creates an index for the secret information and the index is placed in a frame of the video itself. When steganographed by this method, the probability of finding the hidden information by an attacker is lesser when compared to the normal method of hiding information frame-by-frame in a sequential manner.

12. REFERENCES

1. Chae. J. J. and Manjunath .B. S , Jan. 1998 ,"A Robust Embedded Data from Wavelet Coefficients" , University of California, Santa Barbara, CA 93106. vol. 3312, Pp. 308-317.
2. Dominic Bucerzan , 2013 , "Stream cipers analysis method", **International Journal Of Computers Communications & Control** (IJCCC), vol.5 , no.4.
3. Manikandan .R , Uma .M , February 10, 2012 ," Reversible Data Hiding for Encrypted Image," Journal of Computer Applications ISSN: 0974 –p 1925,vol. 5, Issue EICA2012-1.
4. Musbah Aqel .J, Ziad Alqadi .A , Ibraheim El Emary.M , 2007, "Analysis of Stream Cipher Security Algorithm," Journal of Information and Computing Science, ISSN 1746-7659, vol. 2, no. 4, pp. 288-298.
5. Sanjeev kumar, 2011 ,"Quality Assessment of Color Image Compression using Haar Wavelet Transform", **International Journal of Engineering Trends and Technology (IJETT).**vol.3,issue-3.
6. Wei Liu, 2014, "Efficient Compression of Encrypted Grayscale Images", Journal of IEEE Transactions on Image Processing,vol.19.
7. Zhang.X , April 2012," Separable reversible data hiding in encrypted image", IEEE Transactions Information Forencics and Security,7(2):826-832.vol.7, no.5.
8. Zhenxing Qian , 2016 ,"Reversible Data Hiding in Encrypted Images Based on Progressive Recovery", The school of Communication and Information Engineering , Shangai University, China.