International Journal of Recent Research and Review, Vol. VI, Issue 3, December 2013

ISSN 2277 – 8322

Image Steganography Method for Hiding Secret Message in Colored Images by Using IWT

Preeti Chaturvedi[1], R. K. Bairwa[2]

[1]*M.Tech Scholar, Deptt. of CSE, Kautilya Institute of Technology & Engineering, Jaipur (Raj.),India*

[2]*Assistant Professor, Deptt. of CSE, Kautilya Institute of Technology & Engineering, Jaipur (Raj.),India*

Email: preetichobey@gmail.com

***Abstract*- Steganography is a medium to hide the secret message in such a way that only sender and receiver only know about it. No other one on network cannot suspects the existence of the message. The proposed paper represents here a image steganography method for hiding secret message in colored images by using integer wavelet transform. Steganography method is provides more security to images that contain secret message. The proposed techniques uses the LSB technique.**

***Keywords*- Image Steganography, Integer Wavelet Transform, RS Analysis, Genetic Algorithm.**

1. INTRODUCTION

In general, the steganalysis techniques can be categorized into six levels depending on how much information about the hidden messages require. These levels (ordered according to the increased amount of information acquired) are as follows:

a) Differentiation between cover and stego documents—this is the first step in steganalysis and the purpose of this technique is to determine if a given document carries a hidden message.

b) Identification of steganographic method—this technique identifies the type of steganographic method used and it is the so-called multi-class steganalysis.

c) Estimation of the length of a hidden message—this technique reveals the amount of embedded message as the acquired information.

Identification of stego-bearing pixels—this technique uncovers the exact locations where the pixels are used to carry the message bits.

d) Retrieval of stego-key— once the transmitted data which has been already staged reaches to the receiver terminal, and then in order to access the received data a security key is required. This facilitates the authenticity of the data communication. The key is required to access the data. This technique provides access to the stego-bearing pixels as well as the embedding sequence.

e) Message extraction— once the data has been embedded then it becomes available for further transmission or communication. When the transmitted data approaches to the receiver terminal then it is required to be extracted so that the text data being transmitted can be retrieved. The process of extracting the text data from the embedded or stego image is known as message extraction. This technique normally concerns with extracting and deciphering the hidden message to obtain a meaningful message.

In recent research works few algorithms have been proposed which consists of the marginal statistics that are preserved for achieving more security. Previous methods have less data hiding capacity. As we increase the data length distortion increases in the final stego image. The previous methods not strong against the RS attack. All the previous methods provide the basic path to hide the data behind the image. There was no

provision about the increasing capacity of data as no effect on image and how to restrict the RS attack. So this is a big issue in steganography model that how we increase the hiding capacity without any distortion in the image quality and how we provide the security against the RS attack.

The major scopes of this work are listed below.

a) Blind steganalysis: The proposed system has developed a framework in order to distinguish a stego image from a cover image. Mainly, it has been broken several steganographic methods from the literature. Basically this technique uses an image processing technique that take out sensitive statistical data, which employs a better technique to find out the existence of a secret message. Besides, this technique can be impurities and used to identify a different type of steganographic method. These types of identification are important when deal with a new and unknown steganographic method.
b) Use of IWT and GA: The proposed system is extended to determine the best fitness function along with RS analysis to generate the final stego image with hidden message. This is important information that allows a contest to mount a more specific attack. As compared to the literature review, it can be easily analyzed that the proposed system is better to protect from statistical attack.
c) Message length estimation: It has been designed a simple yet effective technique based on first-order statistic to estimate the length of an embedded message. This estimation of the length of message is important and is required if it has been intend to extract a hidden message. It has been identified that the notches and protrusions can be utilized to approximate the degree of image distortion that rose by embedding operation. In practically, this technique attacks the steganographic method that developed in past.
d) Steganographic payload locations identification: It has been presented a technique that identifies the different locations where the hidden message bits can be embedded. This technique is presented in very few researches in the literature that one able to achieve additional secret information. Finally, this additional secret information is important for third party who wants to acquire a hidden message or deceive the communication.

Applications

There are many applications for image digital steganography, including copyright protection, feature tagging, and secret communications [1, 2].

a) Copyright protection*:* A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property [3, 4]. This is the watermarking scenario where the message is the watermark [3, 4]. The “watermark” has a very complex and hard structure. In addition to it, when an image is distributed then an identification of the recipient and time stamp can be embedded to identify the actual pirates. A watermark can also used to find that whether the image has been subsequently modified or not [5]. Detection of an embedded watermark is performed by measuring other quantity characteristic to the watermark in a stego-image. The insertion the watermark and its analysis are required to protect copyrighted material that is responsible for the recent surge of interest in digital steganography and data embedding.
b) Feature tagging: An article, illustration, or poster and other brief explanation elements can be embedded inside an image, for example the names of individual person in a photo or any locations in a map. Copying the stego-image means also copies all of the embedded data and its features. The parties who have the decoding stego-key can able to extract and view the data and features. Another application is an image database in which keywords can be embedded to make easy search engines. If the image is a rigid structure of a video sequence, then timing markers can be embedded in the image for synchronization with audio. An image has been

viewed in number of times can be embedded for “pay-per-view” applications.

Characterizing data hiding techniques

Steganographic techniques embed a message inside a cover. Different-2 features show the strengths and weaknesses of the methods. The respective importance of every feature depends on the particular application [2].

a) Hiding capacity: Hiding capacity is the size of data or information that can be hidden relative to the size of the particular cover. A huge hiding capacity allows the use of a smaller cover for a message of not variable size, so decreases the bandwidth required to transmit the stego-image.
b) Perceptual transparency: The act of hiding the message in the cover force some noise modulation or distortion of the cover image as compare to final image. It is important here that the embedding take place without any degradation or loss of perceptual quality of the cover image. In regarding a secret communications application, if an attacker notifies any distortion (it means suspicion of the presence of hidden data in a stego-image) the steganographic encoding has failed even if the attacker is not able to extract the original message. Maintain the perceptual transparency in an embedded watermark for copyright protection is also importance because the integrity of the original work must be maintained in any circumstances [4]. On other hand for applications in which perceptual transparency of embedded data is not important, than allow more distortion in the stego-image so hiding capacity increases and robustness also, or both.
c) Robustness: Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, for example linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, lossy compression, and conversion from digital to analog form and then reconversion back to digital form (such as in the case when a hard copy of a stego-image is printed and then a digital image is formed by subsequently scanning the hardcopy.) Robustness is important in copyright protection watermarks because pirates will attempt to filter and damaging any watermarks embedded in images [3, 4]. Anti-watermarking software is already available on the Internet and has been shown effective in removing some watermarks [6, 7]. These techniques can also be used to destroy the message in a stego-image.
d) Tamper resistance: Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to change a message once message has been embedded in a stego-image, for example a pirate replacing a copyright mark with one claiming legal ownership. Applications that require high robustness is also require a very strong degree of tamper resistance. In a copyright protection application, good tamper resistance achieving can be hard because a copyright is operative for long years and a watermark must stay resistant to tampering even when a pirate want to modify it by using technology of computing decades in the coming years.

Data embedding

Today’s methods for the embedding of data into cover image divide into three categories: Least-Significant Bit, embedding transforms techniques, and methods that employ perceptual masking.

a) Least significant bit encoding: A digital image consists of a matrix of color and intensity values. In a gray scale image there are 8 bits per pixel are used. In a full-color image there are 24 bits per pixel, and 8 bits assigned to each color components that means red, green and blue. The simplest steganographic techniques embed the bits of the message directly into the least-significant bit of the cover image in a deterministic sequence. Least-significant bit Modulating process does not result in a human-perceptible difference because the amplitude of the change is small. Other techniques “process”

the message with a pseudorandom noise sequence before or during insertion into the image cover. The advantage of LSB embedding is its simple application and other techniques can use these methods [8]. LSB embedding uses the concept of high perceptual transparency. On other hand, there are weaknesses shows when robustness, tamper resistance, and other security issues are take place. LSB encoding is largely susceptible to any type of manipulation of the stego-image. Scaling, rotation, cropping and noise in stego-image are very likely to harm the message. Finally network attacker can easily remove the message by removing the whole LSB plane with little change in the perceptual quality of the modified stego-image. "Steganos" is a LSB embedding system developed in Germany that can embed data inside a variety of image, audio, and text covers [9]. The latest version of the software 1.5 was used below to do the LSB embedding.

b) Embedding transforms techniques: Another class of techniques is embedding the message in a transform domain by modulating coefficients, like as the Discrete-Cosine Transform (DCT), Discrete Fourier Transform, or Wavelet Transform. These transform techniques provides best robustness against lossy compression because they are designed to resist the methods of famous lossy compression algorithms. "Jpeg-Jsteg" software is an example of transform-based steganographic system [8], which embeds the message by modulating DCT coefficients of the stego-image based upon bits of the message and the round-off error during quantization. Steganography that based on transform also offer increased robustness to scaling, rotations or cropping, that depending on the invariant properties of a transform. Spread-spectrum techniques and redundant encoding of the message can be take place in situations where robustness is important [3, 4, 10]. The watermark or message can be thought of as a narrowband signal encoded in a larger frequency band (the cover). By spreading the energy of the embedded message from one side to another, many frequency bands the energy at any particular frequency band is minimize. So the message becomes difficult to detect without destroy the cover. Coding of error correcting can be applied to the message in between embedding to allow recovery even when little areas of the stego-image may be damaged or modified.

c) Perceptual masking systems: Now days, a good deal of research has been reported in extensive the hiding capacity and robustness of steganographic techniques by benefit the properties of the human visual system [3, 4, 11]. The development of accurate human vision models facilitates the design and development of perceptual masking hiding systems [4]. Steganographic techniques designed to be robust to lossy image compression must insert the message into the cover in a way that is perceptually significant. Techniques that processes embed information only in a perceptually insignificant manner, for example LSB techniques for embedding, are exposed to having the embedded data distorted completely. The masking properties of the human visual system allow perceptually significant embedding to be unnoticed by an observer under normal viewing conditions [4]. "Masking" refers to the phenomenon where a signal can be imperceptible to an observer in the presence of another signal (referred to as the masker.) The masking properties are the main reason why it is difficult for one to find a randomly placed needle in a haystack; the needle can be in plain view to an observer (not obscured by any object) yet the observer will have great difficulty locating the needle. Masking (few times known as image-adaptive [4]) systems perform analysis of the image and use the information to determine appropriate regions to place the message data. Analysis can also use by the masking systems to vary the

strength (amplitude) of the embedded data based upon local image characteristics to increase robustness. These types of systems can embed in either the spatial domain or transform domain.

II. PROPOSED SYSTEM

A Data Flow Diagram (DFD) is a graphical representation of the "flow" of data through an information system. Data Flow models are used to show how data flows through a sequence of processing steps. The transformation of data is done at each step before moving on to the next stage. These steps or transformations of data are program functions when Data Flow diagrams are used to document a software design.

The Data Flow Diagram (DFD) for the proposed system can be decomposed into three levels such as level 0, level 1 and level 2.

a) Data flow diagram - level 0

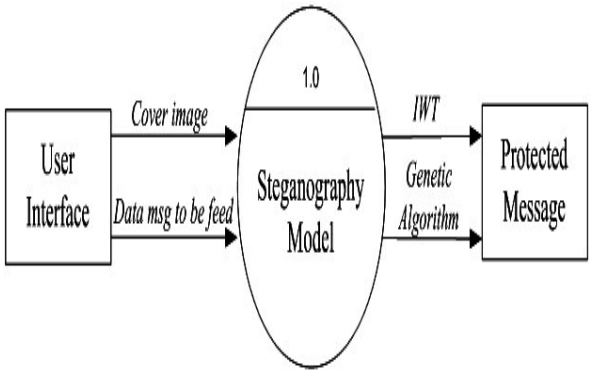


Fig. 1 Level 0 DFD of Proposed Steganography Model

The above diagram represents level 0 data flow diagram of our proposed model of steganography using Inverse Wavelet Transform and genetic Algorithm. The proposed model accepts the input of cover image (original image) from the entity of user interface. The application also uses key for encrypting. Although the final objective is to understand the intensity of RS analysis for the different types of stego images to be used, but for the sake of simplicity, the above figure shows the protected user text message (encrypted) as the obvious outcome of the proposed system.

Considering the overall system architecture and the real time implementation it can be found that the overall system specification and the real time application can be achieved only when all the integrating components are functioning properly.

b) Data flow diagram - level 1

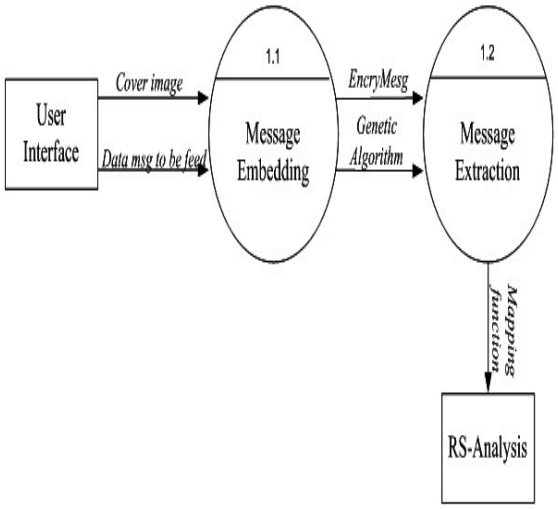


Fig. 2 Level 1 DFD of Proposed Steganography Model

The above diagram represents level 1 data flow diagram of our proposed model of steganography using Inverse Wavelet Transform and genetic Algorithm. So from Fig.3, it can be seen that the main process {1.0} in level 0 is generically classified as two sub-process e.g. Message Embedding {1.1} and Message Extraction {1.2}, where the internal processing using Inverse Wavelet Transform and Genetic Algorithm will lead to design a robust application against RS-analysis. It embeds the secret message in the cover media (e.g. image, audio, video, etc.) to hide the existence of the message. To resist to RS analysis, the influence on the correlation of pixels needs to be compensated. The compensation may be bringing out by adjusting other bit planes. The proposed design presents a new genetic algorithm approach in order to find the best position for data embedding and also optimize the quality of the steganographic image using Inverse Wavelet Transform.

c) Data flow diagram - level 2

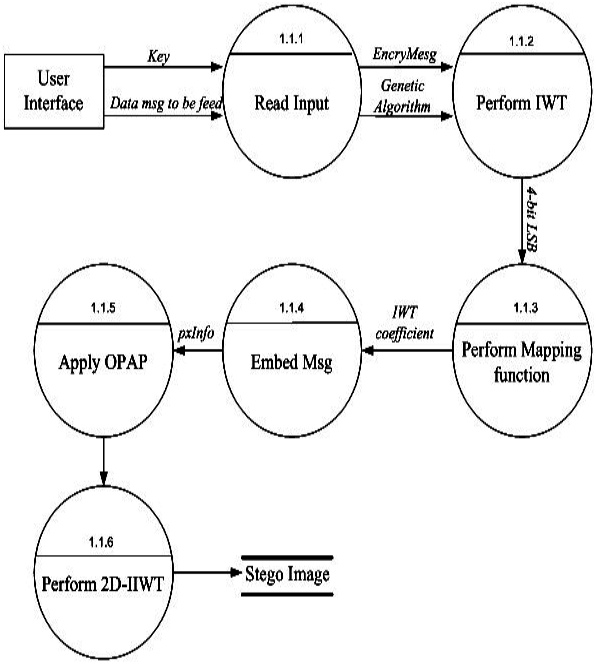


Fig. 3 Level 2 DFD of Proposed Steganography Model

The above diagram highlights the flow of Message Embedding process in the proposed system. The proposed system accepts the input of cover image with user text and key, which is then subjected to IWT followed by mapping function. The user text message is then embedded using OPAP. Two dimensional Inverse Integer Wavelet transform is applied, it is then converts it to stego image, which can be stored in memory then.

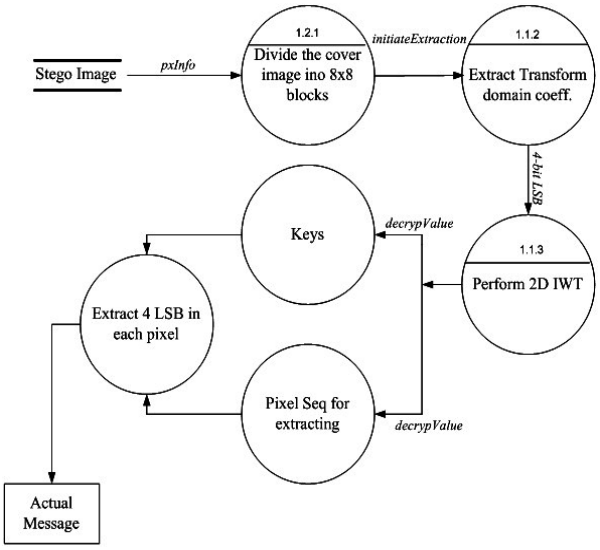


Fig. 4 Level 2 DFD of Proposed Steganography Model

The above figure represents the level 2 data flow diagram of extraction methods used. The process {1.2.1} accepts the input of the stego image, which is then divided into the cover image into 8x8 blocks. Two dimension inverse wavelet transform is extracted by the transforms domain coefficient of each 8x8 blocks. Then the mapping function is employed in the embedding phase and it then provokes to find the pixel sequences for extracting. Finally 4-LSBs in each pixel is extracted to evaluate the actual message.

d) Data flow diagram - level 3

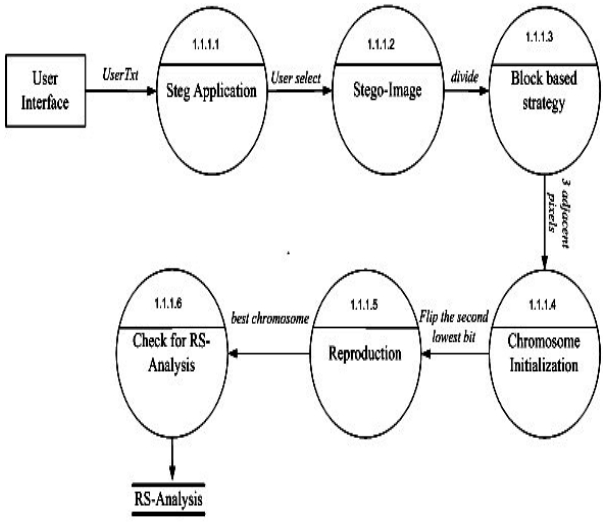


Fig. 5 Level 3 DFD of Proposed Steganography Mode l

The above diagram represents level 3 data flow diagram of our proposed model of steganography using Inverse Wavelet Transform and genetic Algorithm. This paper embeds the message inside the cover with the least distortion therefore we have to use a mapping function to LSBs of the cover image according to the content of the message. We use Genetic Algorithm to find a mapping function for all the image blocks. Local image property can preserve by using block based strategy and reduce the algorithm complexity compared to single pixel substitution. In our GA method, a chromosome is encoded as an array of 64 genes containing permutations 1 to 64 that point to pixel numbers in each block. Mating and mutation functions are applied on each chromosome. Selecting the fitness function is one

of the most important steps in designing a GA-based method. Whereas our GA objective is to improve the quality of image, Pick Signal to Noise Ratio (PSNR) can be an appropriate evaluation test.

III. PROPOSED WORK

This section contains a detailed description of components of software package, components of low-level and other sub-components of the projected work. Module design helps for the implementation of the modules. The modules area unit defined in the projected steganography models is initiated by the structure chart. Module's input needs and outputs generated by the modules area unit delineate during this section.

a) Data embedding:

This is the method flow sheet for data embedding module to illustrate the initiation of security measures at the side of implementation of IWT and Genetic rule. The main purpose of this application is to point out the flow of information embedding operation involved in the process. The frequency domain illustration of the individual created blocks is calculable by 2 dimensional integer ripple transform in order to accomplish 4 sub bands LL1, HL1, LH1, and HH1. One to sixty four genes area unit generated containing the pixels numbers of each 8x8 blocks because the mapping operates. The bits of message in 4-LSBs IWT coefficients each component consistent with mapping functions area unit embedded. Consistent with fitness analysis, optimal component Adjustment process applied on the Image. At the end, inverse 2nd IWT is computed during this module in order to generate the stego image. The input for this process is largely a canopy image and user text message for embedding purpose.

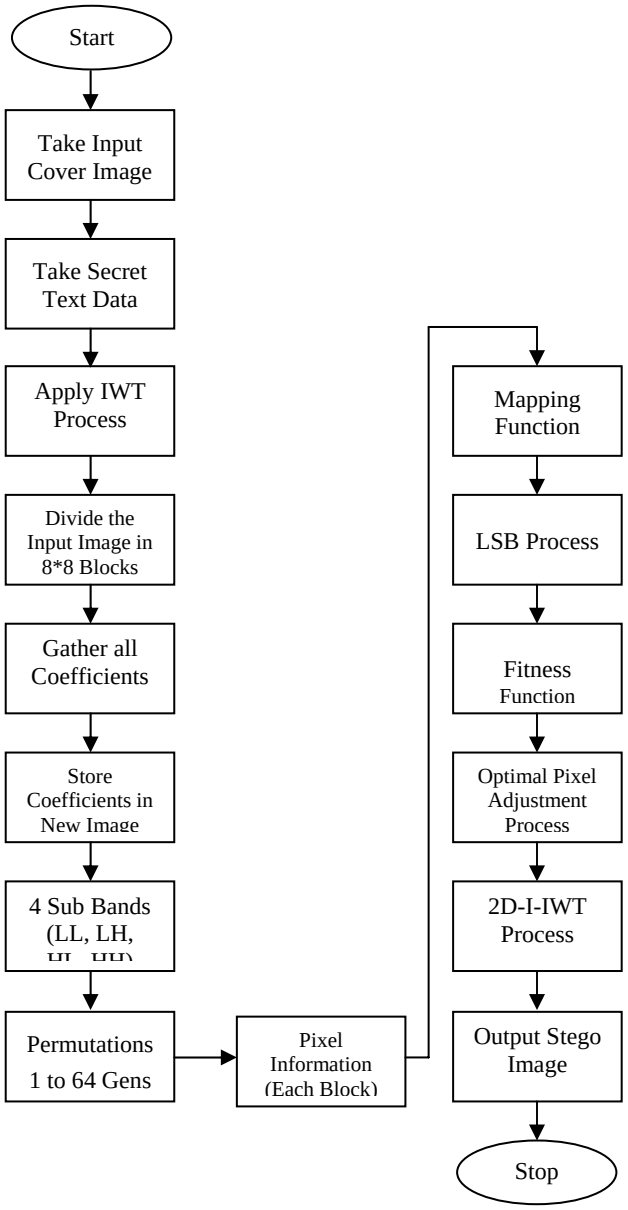


Fig.6 Flow Chart of the Data Embedding process

b) Message extraction

This is the method multidimensional language for message extraction module to illustrate the decipherment hidden text within the stego image. The most purpose of this application is to show the flow of message extraction operation involved within the process. This algorithmic rule primarily takes the input of the generated stego image from the embedding process and applies IWT together with decipherment

key to extract the secret text that has been hidden inside the stego image.

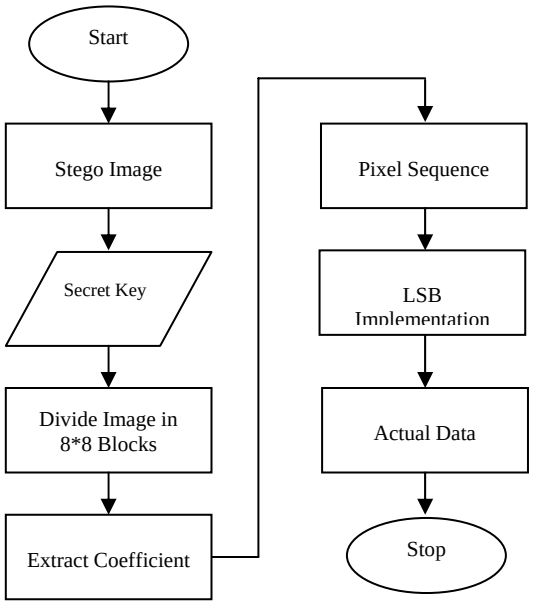


Fig.7 Flow Chart of the Data Extraction process

c) LSB implementation

This method flow chart will show the section wherever LSB is enforced. The most purpose of this method is to indicate LSB implementation. The major operation takes place when the appliance starts getting the size of the cover image and then it creates a tree structure for ease in computation.

IV. IMPLEMENTATION AND RESULTS

The main and necessary phase of a research work is that the implementation of it that shows the particular direction of implementing the state of affairs, methods and step by step development. The implementation half of any development is that the foremost necessary part because it yields the final word solution that solves the matter at hand. The phase of implementation involves the particular materialization of the ideas, that area unit showed within the document analysis and developed within the phase of style. Implementation should be best mapping of the planning document during an appropriate programming language so as to attain the necessary final product. Typically the product is ruined due to incorrect programming language adopted for implementation or unsuitable methodology of programming.

Implementation

Implementation of planned steganography application is usually preceded by necessary selections relating to choice of the platform, the language used, etc. these sort of selections area unit usually influenced by many factors like real environment during which the system works, the speed needed, the safety problems, and implementation related details.

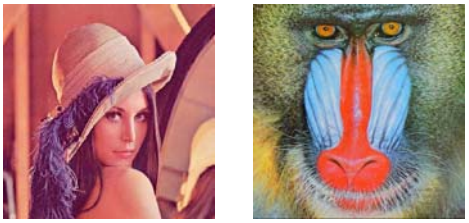
Planned work implementation needs

The implementation of the planned work requires associate input cowl image with a knowledge file for playing the message embedding method. However the software package needs for playing the implementation are:

1. MATLAB 7.10.0.499 (R2010a) or Higher version
2. Microsoft windows XP/7/8
3. .NET framework 3.5 or Higher version

Proposed work Implementation

The proposed implementation of RS-analysis using genetic algorithm for the robust security in Steganography application is done on standard 32-bit windows OS with 1.84 GHz processor and 2 GB RAM. The method is applied on 512x512 colored images “Lena” and “Baboon” as shown in Figure 4.1.



a) Lena b) Baboon

Fig. 8 Input cover image

Experimental result analysis and discussion

The proposed work is done on 2 set of data image as shown in previous section. All the two cover image utilization is 100% and their respective accomplished results of reversible statistical analysis are as follows:

TABLE I
VARIOUS VALUES FOR LENA

For Jet	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.0085433	0.0056553	0.0047631
S_m-S_{-m}	0.0028555	0.012707	0.0092600

TABLE II
VARIOUS VALUES FOR BABOON

For Baboon	Initial Value	After Embedding	After OPAP
R_m-R_{-m}	0.0059921	0.0072314	0.0059856
S_m-S_{-m}	0.0075323	0.010893	0.0029987

Tables I and II are shown various values such as the values of $|R_m-R_{-m}|$ and $|S_m-S_{-m}|$ that represents the RS-steganalysis on regular and singular block. It can be easily seen that the value of $|R_m-R_{-m}|$ and $|S_m-S_{-m}|$ increases from initial value before embedding and after embedding that exhibits a strong correlation in potential of RS-analysis and designed module. At initial stage the values are less, after embedding the message, values increases and finally after applying optimal pixel adjustment process values are decreases. Human visual system is not able to differentiate the colored images with PSNR more than 36 dB. This proposed work embedded the messages in the k-LSBs, from k=3 to k=5 and received a reasonable PSNR. Table III presents the results and it show that for k equal to 4, we have the highest capacity of data hiding and reasonable visual quality. The proposed work embedded the message in the 4-LSBs and received a high PSNR. So, we take k value equal to 4 as the number of bits per pixel. We can increase the capacity up to 5-LSBs. Table III shows the capacity and the PSNR of the proposed method for 4-LSBs. Table IV summarizes the result of four images, Lena-Jet-Baboon and Boat, and compares the PSNR and the capacity of proposed method to one in [12].

TABLE III
Comparison of capacity and PSNR for 4-LSBs

Cover Image	Hiding Capacity (bits)	Data Size (KB)	PSNR (dB)
Lena	2137696 (4-LSBs)	260	56.43
Baboon	2137696 (4-LSBs)	260	60.21

TABLE IV
Comparison of capacity and PSNR obtained from proposed method and the proposed method in [12].

Cover Image	Method	Max. H. C. (bits)	Max H. C. (%)	PSNR (dB)
Lena	Proposed method	2137696	70%	56.43
	An Adaptive steganography technique based on IWT [12]	986408	47%	31.8
Baboon	Proposed method	2137696	70%	60.21
	An Adaptive steganography technique based on IWT [12]	1008593	48%	30.89

V. CONCLUSION AND FUTURE ENHANCEMENTS

In this work we proposed a data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines a data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. The proposed system hide secret data in a random order using a secret key which is only known to both sender and receiver.

The future work should focus on large message embedding, improve the data or message embedding

capacity, security against attacks, hiding techniques apply to audio & video.

VI. REFERENCES

[1] T. Morkel, J.H.P. Eloff, M.S. Olivier, An Overview of Image Steganography, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[2] Domenico Bloisi and Luca Iocchi, Image based steganography and cryptography, International Journal of Computer Applications, 2010.

[3] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy, Implementation of LSB Steganography and its Evaluation for Various File Formats, Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 868-872 (2011).

[4] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, A Survey on Image Steganography and Steganalysis, Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 2, April 2011.

[5] A. Joseph Raphael, Dr. V. Sundaram, Cryptography and Steganography – A Survey, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630, ISSN:2229- 6093, 2010.

[6] Amitava Nag, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar, A Novel Technique for Image Steganography Based on DWT and Huffman Encoding, International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6), 2011.

[7] H S Manjunatha Reddy, K B Raja, High capacity and security steganography using discrete wavelet transform, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6), 2011.

[8] Amin Milani Fard, Mohammad-R. Akbarzadeh, Farshad Varasteh, A New Genetic Algorithm Approach for Secure JPEG Steganography, Engineering of Intelligent Systems, IEEE International Conference, 2006.

[9] Yun Q. Shi, Hyoung Joong Kim, Digital Watermarking, 6th International Workshop, IWDW 2007 Guangzhou, China, December 3-5, 2007, Proceedings Springer, 2008.

[10] Shreelekshmi R, M Wilscy and M Wilscy, Preprocessing Cover Images for More Secure LSB Steganography, International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010.

[11] Taras Holotyak, Jessica Fridrich, and David Soukal, Stochastic Approach to Secret Message Length Estimation in ±k Embedding Steganography, Communications and Multimedia Security 2005.

[12] El Safy, R.O, Zayed. H. H, El Dessouki. A, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", IEEE conference, 2009, pp 111-117.