More Secured Steganography Model with High Concealing Capacity by using Genetic Algorithm, Integer Wavelet Transform and OPAP

Jyoti 1
M.Tech. Scholar, Digital Communication, Rajasthan Technical University-Kota
Department of Electronics & Communication Engineering
Sobhasaria Engineering College, Sikar, Rajasthan, India
E-mail: er.jyotichoudhary@gmail.com

Md. Sabir 2
Assistant Professor
Department of Electronics & Communication Engineering
Sobhasaria Engineering College, Sikar, Rajasthan, India
E-mail: sabii.sankha@gmail.com

Abstract: Steganography is an art of writing for conveying message inside another media in a secret way that can only be detected by its intended recipient. There are security agents who would like to fight these data hiding systems by steganalysis, i.e. discovering covered secret messages and rendering them useless. Steganalysis is the art of detecting the message's existence, message length or place of message where it is to be hidden in covered media and blocking the covert communication. There is currently no more secured steganography system which can resist all steganalysis attacks such as visual attack, statistical attack (active and passive) or structural attack. The most notable steganalysis algorithm is the Reversible Statistical attack which detects the embedded message by the statistic analysis of pixel values. To maintain the security against the Reversible Statistical analysis, the proposed work presents a new steganography model based on Genetic Algorithm using Integer Wavelet Transform. We present a novel approach to resolve such problems of substitution technique of image steganography. Using the proposed Genetic Algorithm and Reversible Statistical analysis Algorithm, the system is more secured against attacks and increases robustness. The robustness would be increased against those attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well. In this proposed work, we studied the steganographic paradigm of data hiding in standard digital images. In recent literature, some algorithms have been proposed where marginal statistics are preserved for achieving more capacity and more security. This proposed system presents a novel technique to increase the data hiding capacity and the imperceptibility of the image after embedding the secret message. In proposed work Optimal Pixel Adjustment Process also applied to minimize the error difference between the cover and stego image. By this work best results have been obtained as compared to existing works. The proposed steganography model reduces the embedding error and provides higher embedding capacity. Detection of message existence will be very hard for those stego images that produced using the proposed method. This work shows the highest embedding capacity and security against Reversible Statistical attack.

Keywords: Genetic Algorithm, IWT, OPAP, RS Analysis.

I. INTRODUCTION

Steganography is the art of hiding information imperceptibly in a cover media. The word "Steganography" is Greek word which means “concealed writing”. Where Stegano means "protected or covered" and graphy - “to write”. Steganography is the art and science of hiding communication; a steganographic system so embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper’s suspicion. In the past, individuals used hidden tattoos or invisible ink to convey steganographic content. Today, personal computer (PC) and network technologies give easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium’s redundant bits (those that can be modified without destroying that medium’s integrity) [3]. The
embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography’s goal is to stay its mere presence undetectable, but steganographic systems, thanks to their invasive nature, leave behind detectable traces within the cover medium. Although secret content is not discovered, the very existence of it is: modifying the cover medium changes its statistical properties, thus eavesdroppers can notice the distortions within the resulting stego medium’s statistical properties. The strategy of finding these distortions is named statistical steganalysis. The purpose of steganography is to hide the presence of communication while the purpose of cryptography is to make the communication incomprehensible by modifying the bit streams using secret keys. The advantage of steganography, over cryptography is that the attackers are not attracted towards communicating messages between sender and receiver while the encrypted messages attract the attackers. Steganalysis is a method of detecting the message hidden in a cover media and to extract it. Changes will be apparent in the statistical property of image if the secret message bits are inserted in image. The strength of the steganography is measured by steganalysis. RS steganalysis is one of the most reliable steganalysis which performs statistical analysis of the pixels to successfully detect the message hidden in the image. However, steganography method to detect the presence of secret message by RS attack/analyzer is difficult in case of color images. Retention of visual quality of the image is also imperative. It is worth to note that genetic algorithm optimizes security and also the quality of the image. It belongs to class of evolutionary algorithms, which imitates the process of natural evolution. The proposed work introduces a genetic algorithm based steganography method to protect against the RS attack in color images.

II. LITERATURE SURVEY
M.F.Tolba, M.A.Ghonemy and A.Taha [4] proposes an algorithm by which the information capacity can reach 50% of the original cover image. It provides high quality of stego image over the existing LSB based method. R. O., El.Sofy and H.H.Zayed [5] provide high hiding capacity up to 48% of the cover image size. In this paper, they have tried to optimize these two main requirements by proposing a novel technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) algorithm.
Ali Al-Ataby and Fawzi Al-Naima [6] propose a modified high capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security.
Souvik Bhattacharya, Avinash Prakash and Gautam Sanyal [7] incorporate the idea of secret key for authentication at both the ends in order to achieve high level of security. In this paper, a specific image based steganography technique for communicating information more securely between two locations is proposed. H. S. Manjunatha Reddy and K. B. Raja [8] propose a high capacity and security steganography using discrete wavelet transform (HCSSD). In this paper the two level wavelet transform is applied as cover and payload. The payload wavelet coefficients are encrypted and fused with wavelet coefficients of cover image to generate stego coefficients based on the embedding strength parameters alpha and beta. Elham Ghasemi, Jamshid and Brahram [9] propose a novel steganography scheme based on Integer Wavelet Transform and Genetic Algorithm. Simulation results show that the scheme outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity i.e. 35.17 dB and 50% respectively.
T. C. Manjunatha and Usha Eswaran [10] use embedding process stores up to 4 message bits in each integer coefficient for all the transform sub-bands. This paper presents a conceptual view of the digital steganography & exploits the use of a host data to hide a piece of information that is hidden directly in media content, in such a way that it is imperceptible to a human observer, but easily be detected by a computer.
Amitav Nag, Sushanta Biswas, Debashree Sarkar and Partha Pratim Sarkar [11] present a technique for image steganography based on DWT. This paper presents a novel technique for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. First, two dimensional Discrete Wavelet Transform (2-D DWT) is performed on a gray level cover image of size M x N and Huffman encoding is performed on the secret messages/image before embedding. Then each bit of Huffman code of secret message/image is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Image quality is to be improved by preserving the wavelet coefficients in the low frequency sub-band also.
Yedla Dinesh and Addanki Purna Ramesh [12] perform a multi-resolution analysis and space frequency localization. As compared to the current transform domain data hiding methods this scheme can provide an efficient capacity for data hiding without sacrificing the original image quality. Saddaf Rubab and M.Younus [13] derive a new algorithm to hide our text in any colored image of any size using wavelet transform. It improves the image quality and imperceptibility. Their method sustains the security attacks. This new method gives better invisibility and security of communication. This method provides double security by involving blowfish, which satisfies the need of imperceptibility.
S.Priya and A.Amsaveni [14] give LSB based edge adaptive image steganography. Edge adaptive stenography on frequency domain improves security and
image quality compared to the edge adaptive stenography on spatial domain.

Rastislav Hovanec, Peter Foris and Dusan Levicky [15] propose a new method of steganography technique based on DWT transform. The proposed method has ability to hide secret message in a digital image. The secret message is embedded into the image by changing wavelet co-efficient. The quality of the stego image of the proposed method is very close to that of the original one. Areezo Yadollahpour and Hossein Miar Naimi [16] proposed a steganalysis technique using auto-correlation coefficients in colour and grayscale images. They suggest that insertion of secret message weakens the correlation between the neighbour pixels and thereby enabling one to detect the message.

Fridrich et al. [17] proposed an effective steganalysis technique popularly known as RS steganalysis, which is reliable even in the detection of non-sequential LSB embedding in digital images.

Andrew D Ker [18] has proposed a general framework for structural steganalysis of LSB replacement for detection and length estimation of the hidden message. He has suggested the use of previously known structural detectors and recommended a powerful detection algorithm for the aforementioned purpose.

Tao Zhang and Xijian Ping [19] have proposed a steganalysis method for detection of LSB steganography in natural images based on different histograms. This method ensures reliable detection of steganography and estimate the inserted message rate. However, this method is not effective for low insertion rates.

Fridrich and Goljan [20] have considered many steganalysis techniques and proposed a steganalysis technique based on image’s biplanes correlation. They state that LSB plane can be estimated from 7 planes out of 8 planes in a pixel of the image. They feel that the performance of the suggested steganalysis method reduces as the LSB plane’s content is further randomized.

Kong et al. [21] proposed a new Steganalysis approach based on both complexity estimate and statistical filter. It is based on the fact that the bits in the LSB plane are randomized when secret bits are hidden in LSB plane.

Amirtharajan et al. [22] proposed a novel and adaptive method for hiding the secret data in the cover image with high security and increased embedding capacity. They feel that by using this method the receiver does not require the original image to extract the information.

Unamaheswari et al. [23] proposed analysis of different steganographic algorithms for secure data hiding. They recommend compressing the secret message and encrypting it with receiver public key along with the stego key. They have analyzed different embedding algorithms and used cryptographic technique to increase the security.

Taras Holotyak e.t. al [24] propose a new method for estimation of the number of embedding changes for non-adaptive ±k embedding in images. The same author [25] has also advocated a new approach to blind steganalysis, based on classifying higher-order statistical features derived from an estimation of the stego signal in the wavelet domain.

Agaiian and Perez [26] propose a new steganographic approach for palette-based images. This recently approach has the advantage of secure data embedding, within the index and the palette or both, using special scheme of sorting. The presented technique also incorporates the use color model and cover image measures, in order to select the best of the candidates for the insertion of the stego information.

Chen and Lin [27] propose a new steganography technique which embeds the secret messages in frequency domain to show that the PSNR is still a satisfactory value even when the highest capacity case is applied. By looking at the results of simulation, the PSNR is still a relaxed value even when the highest capacity is applied. This is due to the different characteristics of DWT coefficients in different sub-bands. Since, the most essential portion (the low frequency part) is kept unchanged while the secret messages are embedded in the high frequency sub-bands (corresponding to the edges portion of the image), good PSNR is not an imaginary result. In addition, corresponding security is maintained as well since no message can be extracted without the “Key matrix” and decoding rules.

Kathryn Hempstalk [28] investigates using the cover’s original information to avoid making marks on the stego-object, by hiding the basic files of electronic reside digital color images. This paper has introduced two image steganography techniques, FilterFirst and BattleSteg. These two techniques attempt to improve on the effectiveness of hiding by using edge detection filters to produce better steganography.

Wang and Moulin [29] provided that the independent and identical distributed unit exponential distribution model is not a sufficiently accurate description of the statistics of the normalized periodogram of the full-frame 2-D image DFT coefficients.

Park e.t. al [30] proposed a new image steganography method to verify whether the secret information had been removed, forged or altered by attackers. This proposed method covers secret data into spatial domain of digital image. In this paper, the integrity is verified from extracted secret information using the AC coefficients of the discrete cosine transform (DCT).

Ramani, Prasad, and Varadarajan [31] proposed an image steganography system, in which the data hiding (embedding) is realized in bit planes of subband wavelets coefficients obtained by using the Integer Wavelet Transform (IWT) and Bit-Plane Complexity Segmentation Steganography (BPCS).

Farhan and Abdul [32] have presented their work in message concealment techniques using image based steganography.

Anindya e.t. al [33] presented further extensions of yet another steganographic scheme (YASS) which is a method based on embedding data in randomized locations so as to resist blind steganalysis. YASS is a technique of
JPEG steganographic that hides data in the discrete cosine transform (DCT) coefficients of randomly chosen image blocks.

Adnan Gutub e.t. al. [34] depicts the random pixel manipulation methods and the stego-key ones in the propose work, which takes the least two significant bits of one of the channels to indicate existence of data in the other two channels. This work showed good results especially in the capacity of the data-bits to be hidden with relation to the RGB image pixels.

Mohammed and Aman [35] used the Least Significant Bits (LSB) insertion method to hide data within encrypted image data.

Aasma Ghani Memon e.t. al. [36] provides a new horizon for safe communication through XML steganography on Internet.

Zaidan e.t. a.l. [37] has presented a model for protection of executable files by securing cover-file without limitation of hidden data size using computation between cryptography and steganography.

Vinay Kumar and Muttoo [38] have discussed that graph theoretic approach to steganography in an image as cover object helps in retaining all bits that participate in the color palette of image.

Wang e.t. al. [39] presented a new steganography based on genetic algorithm and LSB.

In recent research works few algorithms have been proposed which consist of the marginal statistics that are preserved for achieving more security. Previous methods have less data hiding capacity and security against Reversible Statistical attack. As we increase the secret data length distortion increases in the final stego image as compared with cover image. All the previous works provide the basic idea to hide the data behind the image using LSB substitution. There is no idea discussed about the increasing capacity of data so no effect on image and how to ban the RS attack. This is a critical issue in steganography model that how we increase the hiding capacity of an image or cover media without any distortion in the image quality and how to protect the method against the RS attack.

III. PROPOSED SYSTEM ARCHITECTURE

Design is a necessary phases of code development. The design is a methodology throughout that a system organization is established that is able to satisfy the sensible and non-functional system wants. Large Systems are divided into sub-systems that offer few connected set of services. The design process output is an architecture description. With regular analysis and improvement in style of algorithmic program, steganography is taken as a significant meaning to cover information and additionally the current work appears that it is efficient in hiding a large amount of information. GA is applied to realize associate optimum mapping function to cut back the error distinction between the input cover and the stego image and use the block mapping methodology to preserve native image properties and to cut back the complexity of algorithmic program. Optimal pixel adjustment process is applied to increase the hiding capability of this algorithmic program compared to other existing systems.

In this high level system design the whole system design and development is to be administered. The system development with the correct sequence and therefore the synchronization with the all connecting modules measure aiming to be lined within the tactic of high level coming up with. The Genetic algorithm implementation is in addition one of the necessary steps for the high level system design. During this development method the GA has been used for the RS analysis.

Design issues

The proposed work presents a replacement steganographic technique in order to embed large amount of data in colored images whereas keeping the activity degradation to a minimum level using integer wavelet transform (IWT) and Genetic algorithm (GA). This technique permits concealment of a data in uncompressed color image. Our motivation to cover data in images is to provide security to images that contain crucial data. Proposed approach relies on LSB technique which is able to replace more than one bit from every pixel to cover secret message, but the security of the secret data can be improved by combining the least significant bit and wavelet transform. The aim of the design is to plan the solution of a given problem by the document needs. It is the beginning in moving from drawback to the solution domain. The design of the system is the most vital issue affecting the quality of the computer code package and contains a major impact on the coming phases such as testing and maintenance. The proposed work is basically experimental test-bed for analysis of RS-attack using LSB furthermore as genetic algorithm. So the design to be thought of during this work ought to be a framework application in MATLAB in integrated development setting considering all the parameters to protect the data using advance steganography.

Assumptions and dependencies

- The primary assumption of the work is that the user is taking the input of original image and not from any processed or manipulated image.
- The user is predicted to use the standard cryptography algorithmic program in an exceedingly most secure system and network.
- The basic dependency of the work is to run the application, user needs the MATLAB setting and to use application and appraise its basic conception, user needs associate noise free image and knowledge in plain text format solely.

Constraints

The application relies on optimization using genetic rule within the current steganographic applications. Here limitation is that it's been found that whenever a picture input is subjected to such forms of process then there is loss of actual quality of image. So on resist RS analysis, the impact on the relation of pixels must be stipendiary which cannot be achieved by adjusting totally different bit planes. The implementation procedure may be
unworkable in non theoretical application. Therefore to overcome this limitation, GA is applied to calculate the higher adjusting mode that the image quality is not degraded.

**Proposed system architecture**

The planned work ensures the safety against the RS analysis. The application should be designed in such a way so as to overcome all the limitation considered within the previous analysis work. The present aim is to style the architecture of the planned work which depends completely on a sturdy process of safeguarding the input to the application. This strategy incorporates implementing least necessary bit for embedding the key message of the quilt image. Successive issue could be the loss of quality of the image and therefore the planning is done for safeguarding the standard of the image which is achieved by implementing Genetic algorithmic rule. It is a way of search employed in computing to search out exact or approximate solutions to optimization and search issues.

This work presents a completely unique steganography technique which will ultimately increase the capability of data embedding and therefore the imperceptibility of the image after embedding. The proposed system architecture is highlighted as below:

The complete process can be expressed as follows:

![Fig. 2. Complete flow of proposed work](image-url)

The above mentioned figure represents the general system functionalities and the real operative steps of the developed design. In the processing, the program helps so as give a program to handle the developed model and to access the developed module. At the origination, the cover image is selected for embedding the message. Then the text data is to be selected so, as to accomplish the motive of steganography the stego key applied so at the opposite terminal the message can be retrieved by the same key. Once the Key is provided, the real application development for the RS analysis will be started with the strong GA improvement. In this technique, the message is to be embedded in cover image. Genetic algorithm is playing an important role for embedding more and more data in the image. In the architecture of the developed system the integer to integer wavelet transform is applied. Once the message is embedded into the image file, then embedding the image is again recovered so that it is now able to be transmitted over the channel. On the other hand, at the receiver terminal or at the extraction terminal with the accurate stego key, the message is retrieved accurately.

**IV. PROPOSED WORK**

Detailed design of the proposed steganography gives exhaustive image of the foremost parts described in the system design. Meantime this chapter describes the detail design of the system. In this section details and flow chart of each module has been described. The structure chart show control flow, the useful descriptions of that are conferred in the flow chart diagrams.

**Module specification**
The proposed model is prepared by using two fundamental modules:

A) **Embedding module:** The main task of this module is to embed a secret text within the cover colored image using encryption key. The complete cover image is divided into 8x8 blocks before any further processing. The frequency domain representation of the respective created blocks is estimated by two dimensional Integer wavelet transform in order to accomplish 4 sub bands LL1, HL1, LH1, and HH1. This way 1 to 64 genes are generated containing the pixels numbers of each 8x8 blocks of the mapping function. The message bits in 4-LSBs coefficients of IWT in each pixel according to mapping function are embedded. Fitness evaluation based, Optimal Pixel Adjustment Process on the Image is applied. At last, inverse 2D IWT is computed in this module in order to generate the stego image.

B) **Extraction module:** The main task of this module is the extraction of the actual secret text from the stego image to understand the effectiveness of process of message embedding. It takes the stego image as input with key for decrypting the hidden message from the stego image. Once the data has been transmitted over the communication channel and when the receiver receives the embedded image file, then it becomes necessary to again segment the image data and then take out the text data available at the space covered by the text data at the time of message embedding. The extraction can be summarized in a simple sentence as to take out the data that has been embedded.

**Genetic algorithm utilization process**

A Structure Chart (SC) in software engineering and organizational theory is a chart, which shows the deviation of the system configuration to the lowest manageable levels. Steganalysis is the art and science of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography. The objective of steganalysis is to find suspected packages, identified that they have a payload encoded into them or not, and, if it is possible, then resolve that payload. Unlike cryptanalysis, where it is obvious that intercepted data contains a message (though that message is encrypted), generally steganalysis begins with a pile of suspect data files, but few information about which of the files, if anyone, contain a payload of information. The steganalyst is usually something of a forensic statistician, and should begin by minimizing this set of data files (which is often quite large; in a lot of cases, it may be the whole set of files on a computer) to the subset most likely to have been altered. In computing, the smallest amount of important bit (LSB) is that the bit position in a very binary number giving the units price, that is, decisive whether or not the quantity is even or odd. The LSB is usually remarked because the right-most bit, as a result of the convention in number system of writing lesser digit any to the correct. It is analogous to the smallest amount figure of a decimal number, that is that the digit within the ones (right-most) position. A genetic algorithm (GA) is a search technique used in computing to find exact or approximate solutions to optimization and search problems. Genetic algorithms are divided as world search heuristics. Genetic algorithms are a basic category of evolutionary algorithms (EA) that use techniques galvanized by organic process biology like inheritance, mutation, selection, and crossover.

The following figure represents the structural chart representation for the proposed system development. Here it represents the overall processing and the step by step presentation of the proposed work.

![Fig. 3. GA utilization process](image_url)

**Module design**

This section contains a detailed description of components of software, components of low-level and other sub-components of the proposed work. Module
design helps for the implementation of the modules. Module’s input requirements and outputs generated by the modules are described in this phase.

**Data embedding**

This is the process flow diagram for data embedding module to illustrate the initiation of security features along with implementation of IWT and Genetic Algorithm. The main purpose of this application is to show the flow of data embedding operation involved in the process. The frequency domain representation of the respective created blocks is estimated by two dimensional Integer wavelet transform in order to accomplish 4 sub bands LL1, HL1, LH1, and HH1. 1 to 64 genes are generated containing the pixels numbers of each 8x8 blocks as the mapping function. The bits of message in 4-LSBs IWT coefficients each pixel according to mapping functions are embedded. According to fitness evaluation, Optimal Pixel Adjustment Process applied on the Image. At the end, inverse 2D IWT is computed in this module in order to generate the stego image. The input for this processing is basically a cover image and user text message for embedding purpose. Stego image is generated as a output after this process. This module interacts with all the components of the application responsible for selection of parameters for performing encryption.

**Data extraction**

Figure 5 shows the process flow diagram for message extraction module to illustrate the decryption hidden text in the stego image. The main purpose of this application is to show the flow of message extraction operations involved in the process. This algorithm basically takes the input of the generated stego image from the embedding process and applies IWT along with decryption key to extract the secret text which has been hidden inside the stego image. The input for this processing is basically a stego image and decryption key for message extraction purpose. Original user text is generated as output after this process. This module mainly interacts with the previously implemented message embedding process for performing extraction.

**LSB implementation**

Figure 6 shows the flow chart will show the section where LSB is implemented. The major operation takes place when the application starts getting the size of the cover image and then it creates a tree structure for ease in computation. After it gets filter value of the pixels, where the application start the filter and configure the starting and ending bits, that last set the match image. After performing this operation, LSB algorithm will be implemented in the cover image, where the pixels values of the stego-image are modified by the genetic algorithm to keep their statistic characters. Inputs are embedding original message with cover image. Output of the process is actual implementation of LSB algorithm. This module interacts with LSB module and genetic algorithm along with input files of cover image.
Wavelet applications
In mathematics, a wavelet series is an illustration of a square-integrable real number or complex number or complex valued function by a certain orthonormal series generated by a wavelet.

Wavelet transform
Wavelet domain techniques are becoming very popular because of the developments in the wavelet stream in the recent past years. Wavelet transform is employed to convert a spatial domain into frequency domain. The employment of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. A continuous wavelet transform (CWT) is used to divide a continuous-time function into wavelets.

Integer wavelet transform
The proposed algorithm employs the wavelet transform coefficients to embed messages into four subbands of two dimensional wavelet transform. To avoid problems with floating point precision of the wavelet filters, we used Integer Wavelet Transform. The LL subband in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL subband is distorted (figure 7) [9]. Thus Integer Wavelet Transform (IWT) is preferred over Discrete Wavelet Transform (DWT).
wavelet basis on an interval or on an irregular grid, or even on a sphere. The wavelet lifting scheme is a method for decomposing wavelet transform into a set of stages. An advantage of lifting scheme is that they do not require temporary storage in the calculation steps and require less no of computation steps. The lifting procedure consists of three phases: (i) split phase, (ii) predict phase and (iii) update phase.

**Fig. 8. Lifting scheme forward wavelet transformation**

Splitting: Divide the signal \( x \) into even samples and odd samples:

\[
x_{\text{even}} : s_i \leftarrow x_{2i}, \quad x_{\text{odd}} : d_i \leftarrow x_{2i+1}
\]

Prediction: Analyze the odd samples using linear interpolation:

\[
d_i \leftarrow d_i - (s_i + s_{i+1})/2
\]

Update: Update the even samples to maintain the mean value of the samples:

\[
s_i \leftarrow s_i + (d_i + d_{i+1})/4
\]

The output from the \( s \) channel provides a low pass filtered version of the input where as the output from the \( d \) channel provides the high pass filtered version of the input. The inverse transform is obtained by reversing the order and the sign of the operations performed in the forward transform [40].

**Fig. 9. Lifting scheme inverse wavelet transformation**

**Lifting scheme Haar transform**

In the lifting scheme version of the Haar transform, predicts that the odd element will be equal to the even element. The difference among the predicted value (the even element) and the actual value of the odd element replaces the odd element. For the forward transform iteration \( j \) and element \( i \), the new odd element, \( j+1,i \) would be: \( \text{odd}_{j+1,i} = \text{odd}_{j,i} - \text{even}_{j,i} \). In the lifting scheme version of the Haar transform the update step replaces an even element with the average of the even /odd pair (e.g. the even element \( s_i \) and its odd successor \( s_{i+1} \) is \( \text{even}_{j+1,i} = (\text{even}_{j,i} + \text{odd}_{j,i})/2 \). The original value of the odd \( j \) element has been replaced by the difference between this element and its even predecessor. The original value is \( \text{odd}_{j,i} = \text{even}_{j,i} + \text{odd}_{j+1,i} \). Substituting this into the average, we get \( \text{even}_{j+1,i} = (\text{even}_{j,i} + \text{even}_{j,i} + \text{odd}_{j,i})/2 \) [45].

**Genetic algorithm based steganography method**

The proposed method embeds the message inside the cover image with the minimal distortion. Use a mapping function to LSBs of the cover image according to the content of the message. Genetic Algorithm is used to find a mapping function for all the image blocks. Block based strategy preserve local image property and reduces the algorithm complexity as compared to single pixel substitution. The genetic algorithm optimizes the image quality and security of the data.

**Chromosome design**

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. Each chromosome produces a mapping function (figure 10).

**Fig. 10. Chromosome with 64 genes**

Each pixel in a block is considered as a chromosome. Some chromosomes are considered for forming an initial population of the first generation in genetic algorithm. Several generations of chromosomes are created to select the best chromosomes by applying the fitness function to replace the original chromosomes. Reproduction randomly duplicates some chromosomes by flipping the second or third lowest bit in the chromosomes. Several second generation chromosomes are generated. Crossover is applied by randomly selecting two chromosomes and combining them to generate new chromosomes. This is done to eliminate more duplication in the generations. Mutation changes the bit values in which the data bit is not hidden and exchanges any two genes to generate new chromosome. Once the process of selection, reproduction and mutation is complete, the next block is evaluated.

**GA operations**

Mating and mutation functions are applied on each chromosome. The mutation process causes the inversion of some bits and produces some new chromosomes, then, we select elitism which means the best chromosome will survive and be passed to the next generation.

**Fitness function**

Selecting the fitness function is one of the most important steps in designing a Genetic Algorithm based method. Whereas Genetic Algorithm aims to improve the image quality, Peak Signal to Noise Ratio (PSNR) can be an appropriate evaluation test. The fitness function enables to optimize the value through several iterations. Fitness is calculated by the probability of regular and singular groups when positive flipping and negative flipping is applied. Ultimately, the stego-image undergoes RS analysis and the values between original and stego-image are compared.

**Block flipping**
RS steganalysis classifies block flipping into three types. They are positive flipping $F_1$, negative flipping $F_2$, and zero flipping $F_3$. RS steganalysis analyses three primary colors namely red, green and blue individually for color images. Initially, the image is divided into several blocks. Subsequently, flipping functions such as positive flipping and negative flipping are applied on each block of pixels. Later, the variations between original and flipped blocks are calculated. Based on the variation results, the blocks are categorized into regular and singular groups. Let $R_M$ denote relative number of regular group and $S_M$ denote relative numbers of singular groups. According to the statistical hypothesis of the RS steganalysis method in a typical image, the expected value of $R_M$ is equal to that of $R_M$, and the same is true for $S_M$ and $S_M$:

$$R_M \equiv R_M \text{ and } S_M \equiv S_M$$

With application of positive flipping, $R_M$ denotes regular group and $S_M$ is singular group. Similarly, $R_M$ and $S_M$ are regular and singular group when negative flipping is applied. The difference between regular groups, $R_M$ and $R_M$ and the difference between singular groups, $S_M$ and $S_M$ increases with the increase in length of the secret message.

V. IMPLEMENTATION AND EXPERIMENTAL RESULTS DISCUSSION

The important phase of a research work is its implementation which shows the actual direction of implementing the scenario, methods and step by step development. The implementation part of any development is the implementation part as the same yields the ultimate solution, which solves the matter in hand. The phase of implementation involves the actual materialization of the ideas, which are show in the document analysis and are developed in the phase of design. Implementation should be the best mapping of the design document in a suitable programming language in order to achieve the necessary final product. Usually the product is ruined due to incorrect programming language adopted for implementation or unsuitable method of programming. It is better for the phase of coding to be directly connected to the design phase in the sense if the design is in terms of object oriented terms then implementation should be preferably carried out in a object oriented way. The implementation of the system developed has been performed on the MATLAB software platform.

Implementation

Implementation of proposed steganography application is always preceded by important decisions regarding selection of the platform, the language used, etc. These types of decisions are often influenced by several factors such as real environment in which the system works, the speed required, the security issues, and implementation related details. These major implementation decisions are there that have been made before the implementation of the work.

Proposed work implementation requirements

The implementation of the proposed work requires an input cover image with a data file for performing the message embedding process. However the software requirements for performing the implementation are:

- MATLAB 7.10.0.499 (R2010a)
- Microsoft windows XP
- .NET framework 3.5

Guidelines to perform coding

The following guidelines have been used during the implementation of the proposed work:

- Initialize local variables and all pointers initialized to the defined values or NULL.
- Use tracing statements at critical points in the code.
- For all the data types, type definitions are used.
- All the message formats are stored in header file.
- All the functions should not exceed more than 100 lines.
- Function pointers are not used.
- All the codes should be properly indented.
- Use conditional compilation statements, wherever required.

Implementation of algorithm

Data embedding algorithm

The proposed method for data hiding comprises of the following:

- Take the input standard cover image.
- Take the secret text message.
- Apply the secret key (in digits only).
- Perform the Integer Wavelet Transform of the input cover image using lifting scheme.
- Add primal ELS to the lifting scheme.
- Perform integer lifting wavelet transform on image.
- Divide the input cover image in 8x8 blocks.
- Select any of the wavelet coefficients (redundant coefficients) from the obtained high frequency coefficients.
- Generate 64 genes containing the pixels numbers of each 8x8 blocks as mapping function.
- Initialize empty matrix to store the wavelet values.
- Obtain 8x8 blocks for R G B.
- Concatenate all coefficients together.
- Store the coefficient in new image.
- Embed in K-LSBs IWT coefficients in each pixel according to mapping function.
- Select any one of the pixels from RGB.
- Now the selected coefficients are processed to make it fit for modification or insertion.
- Fitness evaluation is performed to select the best mapping function.
- The secret message plus the message length is embedded into the processed coefficients.
- This modified coefficient is now merged with the unmodified coefficients.
- Calculate embedded capacity.
- Apply Optimal Pixel Adjustment Process on the image.
The proposed method for data extraction comprises of the following:
- Take the desired stego image.
- Apply the same secret key as given in embedding process.
- Divide the stego image into 8x8 blocks.
- Extract the transform domain coefficient by 2D IWT of each 8x8 blocks.
- Find the pixel sequences.
- Select the desired pixels for process.
- Extract K-LSBs in each pixel.
- Process the selected pixels coefficient to make it fit, for extraction.
- Now extract the message length and the secret message from these processed coefficients.
- Secret message to be obtained.

**Data extraction algorithm**
The proposed method for data extraction comprises of the following:
- Take the desired stego image.
- Apply the same secret key as given in embedding.
- Divide the stego image into 8x8 blocks.
- Extract the transform domain coefficient by 2D IWT of each 8x8 blocks.
- Find the pixel sequences.
- Select the desired pixels for process.
- Extract K-LSBs in each pixel.
- Process the selected pixels coefficient to make it fit, for extraction.
- Now extract the message length and the secret message from these processed coefficients.
- Secret message to be obtained.

**RS-analysis algorithm**
The proposed method for RS analysis comprises of the following:
- Create function for non-negative flipping (Fp).
- Change LSB as per flipping.
- Initialize Relative number of regular block after positive flipping (R+) = 0.
- Initialize Relative number of Singular block after positive flipping (S+) = 0.
- Divide Stego Image into 8x8 blocks.
- For a modified block B, apply the non-positive flipping B+ and the non-negative flipping B− on the block. The flipping mask M+ and M− are generated randomly. The result is B'+ and B'−.
- Estimate F (B+), F (B−) and F (B).
- Define four variables to divide the blocks by comparison of F (B+), F (B−) and F (B).
- Initially P+ = 0, P− = 0, P+ = 0 and P− = 0.
- Do the following steps for 100 times
  - For nn = 1:100
    - Apply the non-positive flipping B−.
    - Fp = non_positive_flipping (B).
    - Apply non-negative flipping F+.
    - Fp = non_negative_flipping (B).
    - Calculate f (B+), f (B−) and f (B).
    - C = calculate_correlation (B).
    - Correlation for non positive flipping.
    - Cn = calculate_correlation (Fp).
    - Correlation for non positive flipping.
    - Cp = calculate_correlation (Fp).
    - Estimate P−, the count of the occurrence when the block is regular under the non-negative flipping.
    - Estimate P+, the count of the occurrence when the block is singular under the non-negative flipping.
    - Estimate P−, the count of the occurrence when the block is regular under the non-positive flipping.
    - Estimate P+, the count of the occurrence when the block is singular under the non-positive flipping.
    - If Cn > C, then increase P− (Regular).
    - P− = P− + 1.
    - Else, increase P+ (Singular).
    - P+ = P+ + 1.
    - End
    - If Cp > C, then increase P+ (Regular).
    - P+ = P+ + 1.
    - Else, increase P− (Singular).
    - P− = P− + 1.
    - End
    - Compare P− to P+ and P− to P−, the block’s label are determined, str = [1].
    - If P+ / P− > 1.8, then str = ‘R+’.
    - disp (‘R+’), Label of the block ‘R+’.
    - Rp = Rp + 1.
    - End
    - If P− / P+ > 1.8, then str = ‘S+’.
    - disp (‘S+’) , Label of the block ‘S+’.
    - Sp = Sp + 1.
    - End
    - If P− / P− > 1.8, then str = [str ‘R−’].
    - disp (‘R−’), Label of the block ‘R−’.
    - Rm = Rm + 1.
    - End
    - If P+ / P− > 1.8, then str = [str ‘S−’].
    - disp (‘S−’), Label of the block ‘S−’.
    - Sm = Sm + 1.
    - End
  - At last, the blocks are categorized into 4 groups (R+R−), (R+S−), (S+R−), (S+S−).
  - Reject the block which doesn’t fall in 4 groups.
  - Now use genetic algorithm for minimizing R-block.
  - The blocks, which are not included in the 4 categories, are not processed in following steps. Compared to the original image, the values of R+ R− and S+ S− blocks are increased in the stego-images. This phenomenon can be detected by the RS analysis. The main aim of the proposed algorithm is to decrease the amount of R− blocks. Therefore genetic algorithm is deployed to adjust them to maintain the visual quality of image as given in follow section.

**Optimization technique or genetic algorithm**
The proposed method for genetic algorithm comprises of the following:
- Perform Chromosome Initialization Steps.
- From the first pixel, select every 4 pixels.
- B1 = B (:)
- crossover = 0.
- Initialize Alpha as 0.88.
implementation of RS...

If Cn > C, then Regular.

Cn = calculate_correlation (Fn).

Correlation for non positive flipping.

Calculate f (B0+), f (B0-), and f (B).

C = calculate_correlation (B).

Correlation for non positive flipping.

Cn = calculate_correlation (Fn).

If Cn > C, then Regular.

P_S = P_S + 1.

Else, Singular.

P_S = P_S + 1.

End

If Cp > C, then Regular.

P_r = P_r + 1.

Else, Singular.

P_S = P_S + 1.

End

iff1 = abs (P_sR - P_r).

iff2 = abs (P_sS - P_s).

If difference is more than 5% then.

iff1 > 0.05*iff2.

Successful then replace.

I (ii:ii+7, jj:jj+7) = reshape (B1, 8, 8).

Successful then replace.

If diff1 > 0.05*diff2.

End

Successful then replace.

<table>
<thead>
<tr>
<th>Image 351x333 to 431x415</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena (JPG, 512x512)</td>
</tr>
<tr>
<td>Fig. 11. Input cover images</td>
</tr>
</tbody>
</table>

Experimental result analysis and discussion

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

<table>
<thead>
<tr>
<th>Table 1</th>
<th>VARIOUS VALUES FOR LENA IMAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Lena</td>
<td>Initial Value</td>
</tr>
<tr>
<td>R_m-R_m</td>
<td>0.0097783</td>
</tr>
<tr>
<td>S_m-S_m</td>
<td>0.0029662</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2</th>
<th>VARIOUS VALUES FOR BABOON IMAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Baboon</td>
<td>Initial Value</td>
</tr>
<tr>
<td>R_m-R_m</td>
<td>0.0059805</td>
</tr>
<tr>
<td>S_m-S_m</td>
<td>0.0076634</td>
</tr>
</tbody>
</table>

The tables 1 and 2 have shown the values of $|R_m-R_m|$ and $|S_m-S_m|$ that represent the RS-steganalysis on the regular and singular block. It can be 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 the 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 decreasing. 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, for k=4 and have received PSNR more than 40 (Table 3) which is considered to be a good achievement.

TABLE 3
COMPARISON OF HIDDING CAPACITY AND PSNR FOR 4-LSBS

<table>
<thead>
<tr>
<th>Cover Image</th>
<th>Hiding Capacity (bits)</th>
<th>Data Size (KB)</th>
<th>PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>2137696 (4-LSBs)</td>
<td>260</td>
<td>46.83</td>
</tr>
<tr>
<td>Baboon</td>
<td>2137696 (4-LSBs)</td>
<td>260</td>
<td>49.65</td>
</tr>
</tbody>
</table>

Figure 12 shows the images after embedding with 4-LSBs. As we compare these embedded images with the input cover images (figure 11), we realize that there are no significant changes in images. The embedded images look like the same as cover images. So the attackers cannot realize in between the communication of two parties that secret message is embedded in these images.

VI. CONCLUSIONS
Steganography is a method that provides secret communication between two parties. It is the science of hiding a data, message or information in such a secure way that only the sender and recipient are aware about the presence of the message. The main advantages of this type of secure communication or we can say steganography is that it does not make any attention about the message to attackers or we can say does not attract the attackers. Strongest steganalysis method which is known as RS analysis detects the secret hidden message by using the statistical analysis of pixel values. The main aim of this work is to develop a steganography model which is highly RS-resistant using Genetic algorithm and Integer Wavelet Transform. This proposed work introduces a novel steganography technique to increase the capacity and the imperceptibility of the image after embedding. This model enables to achieve full utilization of input cover image along with maximum security and maintains image quality. GA employed to obtain an optimal mapping function to lessen the error difference between the cover and the stego image and the use the block mapping method to preserve the local image properties. In this proposed method, the pixel values of the stego image are modified by the genetic algorithm to retain their statistical characteristics. So, it is very difficult for the attacker to detect the existence of the secret message by using the RS analysis technique. We have applied the OPAP to increase the hiding capacity of the algorithm in comparison to other established systems. However, the computational complexity of the new algorithm is high. Further, implementation of this technique improves the visual quality of the stego image which is almost same as the input cover image. But, as we increase the length of the secret message, the chance of detection of secret hidden message by RS analysis also increases. The simulation results show that capacity and imperceptibility of image has increased simultaneously. Also, we can select the best block size to reduce the computation cost and in order to increase the PSNR using optimization algorithms such as GA. However, future works focus upon the improvement in embedding capacity and further improvement in the efficiency of this method.

Future scope
This proposed work is restricted to specific functionality only. The proposed work in this dissertation has been experimented on a single computer system and not on any network. Standard input cover image is only used in this steganography module. Proposed method is not applicable on audio, video and other biometrics etc. Large message steganography cannot be performed as the embedding capacity is confine to the data feed. Future work can be performed on the following:

- Improvement in data embedding capacity and more security against all types of attacks.
- Security design experimented over multiple computers / network.
- The data hiding technique can be applied to video, speech and other biometrics.
- Protection of the system against histogram attack.

REFERENCES


[34] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi, “Pixel indicator high capacity technique for RGB image based steganography”, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications,


