A

Project Report

On

“TECHNIQUE OF HIDING PRIVATE OR SENSITIVE INFORMATION WITHIN AN IMAGE”

SUBMITTED IN THE PARTIAL FULFILLMENT OF THE

REQUIREMENT FOR THE AWARD OF THE DEGREE OF

**BACHELOR OF TECHNOLOGY**

In

Computer Science and Engineering

Submitted by: -

**SHUBHAM KUMAR SHARMA (12500115100)**

**SHUVENDU SANDILYA (12500115096)**

**VIJAY KUMAR YADAV (12500115122)**

Under the esteemed guidance of

**Ms. Bidisha Roy**

**Assistant Professor**

Dept. of CSE



**Department Of Computer Science and Engineering**

**Bengal College of Engineering and Technology**

Durgapur, W.B



Department of Computer Science and Engineering

**Bengal College of Engineering and Technology**

Durgapur, W.B

**CERTIFICATE OF APPROVAL**

The project entitled **“****TECHNIQUE OF HIDING PRIVATE OR SENSITIVE INFORMATION WITHIN AN IMAGE”** submitted by **Shubham kumar Sharma** **(12500115100), Shuvendu Sandilya (12500115096)** and **Vijay kumar** **Yadav** **(12500115122)** under the guidance of “**Ms. Bidisha Roy**” **Assistant professor** is here by approved as a creditable study of engineering subject to warrant its acceptance as a pre-requisite to obtain the degree for which it has been submitted. It is understood that by this approval the undersigned don’t necessarily endorse or approve any statement made, opinion or conclusion drawn therein but approve the project only for the purpose for which it is submitted.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Ms. Bidisha Roy SK ABDUL RAHIM Assistant Professor** (Head of the department)

Computer science and engineering



**Department of Computer Science and Engineering**

**Bengal College of Engineering and Technology**

Durgapur, W.B

**UNDERTAKING**

We, **Shubham kumar Sharma** **(12500115100), Shuvendu Sandilya (12500115096)** and **Vijay kumar** **Yadav** **(12500115122)** B. Tech, 8th Semester (Computer Science and Engineering), hereby declare that our project report, entitled “**TECHNIQUE OF HIDING PRIVATE OR SENSITIVE INFORMATION WITHIN AN IMAGE**” is our own contribution. The work or ideas of other people which are utilized in this report has been properly acknowledged and mentioned in the reference. We undertake total responsibility if any traces of plagiarism are found at any later stage.

**Shubham kumar Sharma (12500115100)**

**Shuvendu Sandilya (12500115096)**

**Vijay kumar Yadav (12500115122)**

**ACKNOWLEDGEMENT**

This project has been done in the partial fulfilment for the award of the Degree of B. Tech in Computer Science and Engineering under the official permission of **Ms. Bidisha Roy**, **Assistant professor** of Department of Computer Science and Engineering, BCET, Durgapur. During this phase we have done a lot of research in this subject. We would also like to thank our mentor, for his constant guidance and support throughout the completion of this project. We could not have completed this project without his help.

Secondly, we do not miss a chance to thank our esteemed HOD **Sk. Abdul Rahim** and all other faculty members who have provided us with the informative knowledge which was a great help in completion of this project.

This project would not have been successful without the help of the above-mentioned authorities.

Place: BCET, DURGAPUR

Shubham Kumar Sharma (12500115100)

Shuvendu Sandilya (12500115096)

Vijay Kumar Yadav (12500115122)

Date:

**CONTENTS**

**TOPIC PAGE NO**

1. INTRODUCTION 1

1. APPLICATIONS 3
2. DATA FLOW DIAGRAM 7
3. PROPOSED WORK 12
4. IMPLEMENTATION 15
5. RESULTS AND DISCUSSION 16
6. FUTURE SCOPE 22
7. CONCLUSION 24
8. REFRENCES 26

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| S.NO | FIGURES NAME | PAGE.NO |
| 1.  2.  3.  4.  5.  6.  7.  8.  9.  10.  11. | Level 0 DFD of Proposed Steganography Model  Level 1 DFD of Proposed Steganography Model  Level 2 DFD of Proposed Steganography Model  Level 3 DFD of Proposed Steganography Model  Flow Chart of the Data Embedding process  Flow Chart of the Data Extraction process  Cover Image  Text File Containing The Information  Cover Image After Applying DWT   1. Steg Image (b) Data Hiding Message   (a) Data Retrieving Message (b) Decoded Text | 16  17  18  20  22  23  25  26  27  28  29 |
|  |

**ABSTRACT**

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

**CHAPTER I**

**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:

1. Differentiation between cover and stegno 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.
2. Identification of steganographic method—this technique identifies the type of steganographic method used and it is the so-called multi-class steganalysis.
3. Estimation of the length of a hidden message— this technique reveals the amount of embedded message as the acquired information. Identification of stegno-bearing pixels this technique uncovers the exact locations where the pixels are used to carry the message bits.
4. Retrieval of stegno-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 stegno-bearing pixels as well as the embedding sequence.
5. 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 stegno 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 stegno 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 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.**

1. **Blind steganalysis**: The proposed system has developed a framework in order to distinguish a stegno 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.
2. **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 analysed that the proposed system is better to protect from statistical attack.
3. **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.
4. **Steganographic payload locations identification:** It has been presented a techniquethat identifies the different locations where thehidden message bits can be embedded. Thistechnique is presented in very few researches inthe literature that one able to achieve additionalsecret information.

**CHAPTER II**

**APPLICATIONS**

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

1. **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 use 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 stegnoimage.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.
2. **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].

1. **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.
2. **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, then allow more distortion in the stego-image so hiding capacity increases and robustness also, or both.
3. **Robustness:** Robustness refers to the ability of embedded data to remain intact if the stegnoimage 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.
4. **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 stegnoimage, 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 wants 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.

1. **Least significant bit encoding:** A digital image consists of a matrix of colour and intensity values. In a grey scale image, there are 8 bits per pixel are used. In a full-colour image there are 24 bits per pixel, and 8 bits assigned to each colour 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 stegno-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 an 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.
2. **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 stegno-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 taken 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.
3. **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.

**CHAPTER III**

**DATA FLOW DIAGRAM**

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.

1. **Data flow diagram - level 0**



**Fig 3.1 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.

1. **Data flow diagram - level 1**



**Fig 3.2 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.

1. **Data flow diagram - level 2**



**Fig 3.3 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 converting it to stego image, which can be stored in memory then.



**Fig 3.4 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 transform’s 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.

1. **Data flow diagram - level 3**



**Fig 3.5 Level 3 DFD of Proposed Steganography Mode**

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.

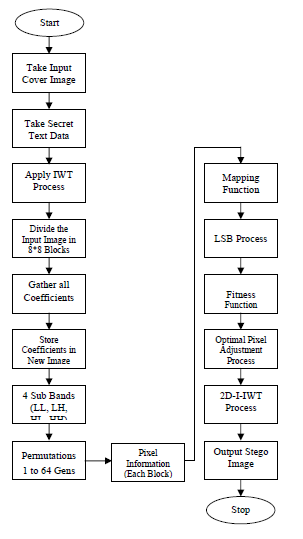
**CHAPTER IV**

**PROPOSED WORK**

This section contains a detailed description of components of software package, components of lowlevel 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.

1. **Data embedding: -**

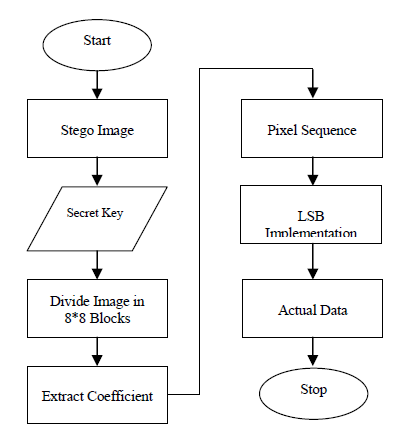
This is the method flow sheet for data embedding module to illustrate the initiation of security measures at the side of implementation of IWT and Genetic rule. The main purpose of this application is to point out the flow of information embedding operation involved in the process. The frequency domain 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 4.1 Flow Chart of the Data Embedding process**

1. **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 4.2 Flow Chart of the Data Extraction process**

1. **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.

**CHAPTER V**

**IMPLEMENTATION**

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 choose of the platform, the language used, etc. these sorts 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

CHAPTER VI

**Result and discussions**

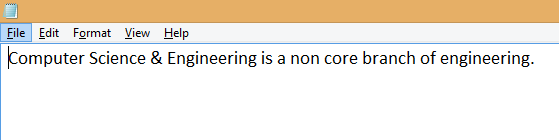
MATLAB 9.2.0.5 is used to perform this project on securing information exchange using image processing. This entire project consists of two phases. First phase determines how a text file is encoded within an image and second phase determines how the text file is decoded from that image. All the elements used in this project including codes, image and the text file to be secured are enclosed within a single folder.

**6.1** **ENCODING TEXT FILE WITHIN AN IMAGE**

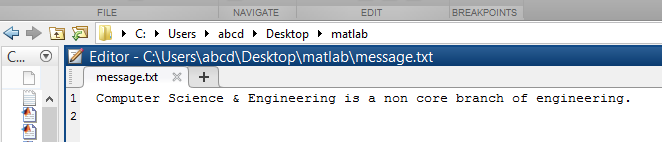
# **Screenshot (69)**

# fig 6.1 COVER IMAGE

The cover image (FIG 6.1) represents the original image that is used in the project within which the information to be exchanged is to be hide.



(a)

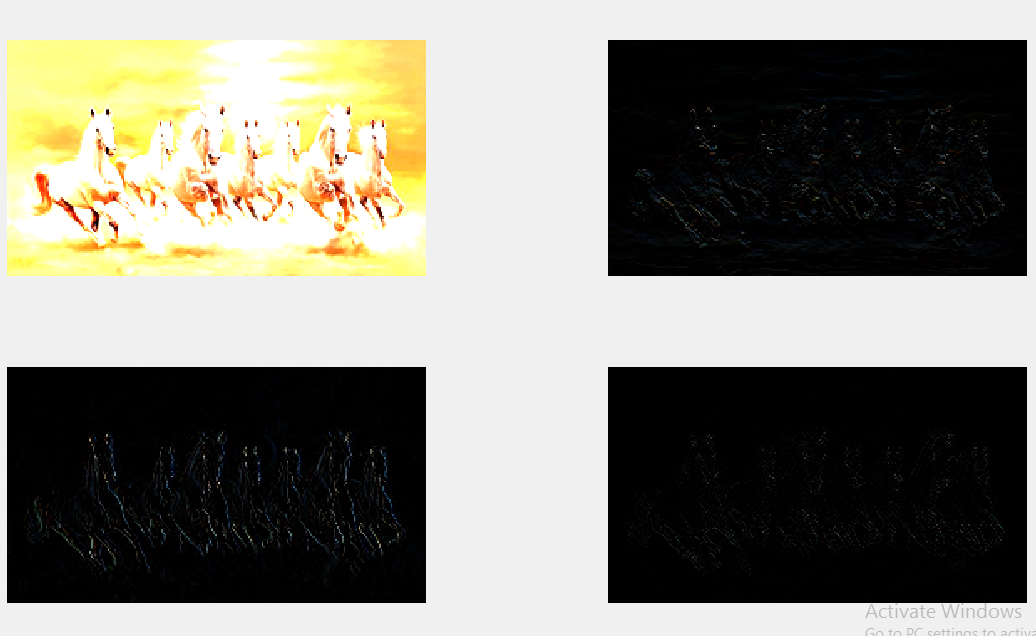


(b)

FIG 6.2 TEXT FILE CONTAINING THE INFORMATION

The information that is to be secured while exchanging over internet is firstly generated in a notepad (FIG 6.2(a)). Then that information is stored in a text file with .txt extension in the MATLAB folder (FIG 6.2(b)).

In order to hide the text file in the cover image, discrete wavelet transform (DWT) technique is applied on the cover image. After applying this technique, the cover image gets divided into four different channels as shown in FIG 6.3.



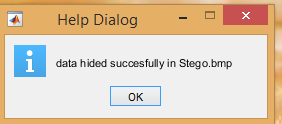
FIGS 6.3 COVER IMAGE AFTER APPLYING DWT

In these four channels the first channel contains the least noise (almost negotiable) and the last channel is the noisiest one. So, no manipulation is done in the first channel and the entire text file will be stored in rest three channels.

In the second channel the length and maximum ASCII value of the information inside the text file is stored. Then half of the information is stored in third channel and the rest half information is stored in the last channel. After hiding the entire information, the inverse discrete wavelet transform technique is applied to reconstruct the cover image. Now the reconstructed cover image will be known as stego image (FIG 6.4(a)) and finally the message for successful data hiding will be displayed (FIG 6.4 (b)).



(a)

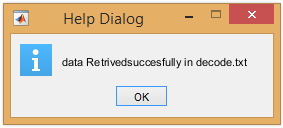


(b)

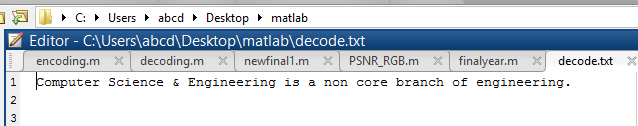
FIG 6.4 (a) STEGO IMAGE (b) DATA HIDING MESSAGE

**6.2 DECODING TEXT FILE FROM AN IMAGE**

After successfully hiding the text file in an image now the question arises on how to decode it. So, to decode the text file from the image, again discrete wavelet transforms (DWT) technique is used on stego image (FIG 6.4(a)). Again, the image is divided into four channels and then one by one information stored in each channel will be retrieved. Then the successful decoded data message will be displayed (FIG (6.5(a)). The decoded data is then stored in a new text file in MATLAB. On comparing the decoded data (FIG (6.5(b)) with the original data (FIG 6.2(b)), we see that both the data are exactly same. Hence the recovery of data is 100% accurate.



(a)



(b)

FIG 6.5 (a) DATA RETRIEVING MESSAGE (b) DECODED TEXT

**TABLE 6.3 RESULT OF THE PROJECT ON DIFFERENT TYPES OF IMAGES**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **COVER IMAGE** | | **FORMAT** | **ORIGINAL TEXT** | **STEGO IMAGE** | **PSNR** | **RECOVERED IMAGE** |
| Screenshot (62) | .jpg | | Screenshot (77) | Screenshot (62) | 173 | 100% |
| Screenshot (78) | .bmp | | Screenshot (77) | Screenshot (78) |  | 100% |
| Screenshot (79) | .png | | Screenshot (77) | Screenshot (79) |  | 100% |

**FUTURE SCOPE**

In this work it explores only a small part of the science of steganography. As a new discipline, there is a great deal more research and development to do, the following section describe areas for research which were offshoots of, or tangential to, our main objectives.

1. **Detecting Steganography in Image Files**

Can steganography be detected in images files? This is difficult question. It may be possible to detect a simple Steganographic technique by simple analysing the low order bits of the image bytes. If the Steganographic algorithm is more complex, however, and spreads the embedded data over the image is random way or encrypts the data before embedding, it may be nearly impossible to detect.

1. **How widespread is the Use of Steganography?**

If a technique or set of techniques could be devised to detect steganography, it would be interesting to conduct a survey of images available on the internet to determine if steganography is used, by whom and for what purposes. Steganographic applications are available on the Internet, but it is not known if they are being used.

1. **Steganography on the World Wide Web**

The world wide web(www) makes extensive use of inline images. There are literally millions of images on various web pages worldwide. It may be possible to develop an application to serve as a web browser to retrieve data embedded in web page images. This “stego-web” could operate on top of the existing WWW and be a means of covertly disseminating information.

1. **Steganography in printed media**

If the data is embedded in an image, the image printed, then scanned and stored in a file can the embedded data be recovered? This would require a special form of a steganography to which could allow for in accuracies in the printing and scanning equipment.

1. **Anti-steganography measures**

As was seen in this thesis, JPEG garbles any unencoded steganographically embedded data. Also, palettization (mapping a large number of colours in an image to a smaller subset of colours) of an image will it unsuitable for steganography. It is likely, as with JPEG, that some means may be employed to prevent loss of steganographially embedded data when its wrapper file is processed. The question remains open as to what is the most effective anti-Steganographic tools or set of tools.

**CONCLUSION**

To hide confidential information steganography can be effectively used. The objective of any Steganographic method is to hide maximum secret information which is immune to external attacks and also should not convey the fact that the cover medium is carry secret information. This thesis has used LSB substitution technique for time domain and different transforms for frequency domain.

The random key made use of while LSB technique is employed has proved to be better than simple LSB substitution. When the personal is key is made use of in the techniques have not altered the resolution of the image much and appears to be negligible as been seen with the obtained results. Hence the hidden data getting damaged buy the third person is almost impossible. The algorithm can be implemented in both grayscale and color image since it has made use of 8 bit and 24bit images of size for both cover and secret image.

In Spatial domain methods one can get high payload capacity. The edge detection techniques which are used in the current methods do not recognizes the shades of the edge region, which can also be considered to embed the extra bits. The number of edge pixels can be increased by identifying the edges and shades of edges.

The Transform domain methods are highly robust. They embed the message bits in the regions which are highly insensitive to compression, filtration or transformation. But their payload capacity is low. Also, the visual qualities of the Stego-image are poor. Spatial domain is better compared to transform domain. In Spatial Domain techniques simple LSB substitution methods are less secure and payload capacity is less. To increase security Randomization techniques are used. These methods spread the message randomly into the cover image but payload capacity is still less. Edge detection method increases the payload capacity and it improves randomness and hence security. As discussed, the current edge detection methods do not recognize the shades of the edge region which are also capable of embedding more bits with less distortion. The shades of the edges are detected by Multiple Edge Detection method. In Multiple Edge Detection method, the edge detection method is applied for 2-3 times which increase the number of edge pixels. As the number of edge pixels is increased more data can be hidden in to the cover image. To add randomness to the embedding procedure which increases security, Variable Embedding can be employed in which a suitable embedding ratio is chosen and according to that the message bits are embedded into the image pixels. The increase in the payload decrease PSNR value, which indicates image degradation amount. To improve PSNR Minimum Error Replacement [MER] method is used. In this method the next higher bit than the last embedded bit is toggle to decrease the pixel error.

Stego and crypto way shows new way of embedding the data, especially in Multiresolution analysis, there are different ways of getting Multiresolution; this thesis has made use of Multiresolution analysis on wavelets and Curvelets. The experimental analysis has proved that Curvelets is the best Multiresolution transformation available. This work has been implemented with the library which has an accuracy of 15 fractional digits. The results obtained have a good PSNR value, along with the crypto style of embedding.

Steganography is to create secrete communication, in addition to this crypto way of embedding gives us higher end of security. Even if the person gets both stego and cove image he needs key to retrieve the data, without the key one can’t recover the data. Thus, additional security is incorporated to the normal Steganography technique.

Image steganography is successfully obtained for different embedding techniques in both wavelet and curvelet domain. Depending on the demand of the application one can choose any of the techniques developed. The simulations are performed in MATLAB 7.7.0(R2008b) and PSNR are calculated. It is found that Curvelet is a better approach than wavelet transformation. In this work data embedding is done by considering block of size 85\*85.

In the frequency domain technique use of skin tone algorithm has given very good results. The proposed method uses skin tone detection for finding skin portion of image and within this skin portion secret data embedding is done using DWT domain. Four cases of embedding are considered. It is observed that hiding of secret data in only the cropped skin portion enhances the security. And according to result and discussion proposed scheme provides good image quality in all four cases.

In Transform domain methods the pay load capacity is low and the future scope is to enhance Stego image quality and payload capacity. The payload capacity can still be increased by embedding more bits into edge pixels and less to non-edge pixels. Future Enhancement can be done by embedding data pixel by pixel, thus increase in the payload can be attained.

**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, (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 Fredrich, and David Soukal, Stochastic Approach to Secret Message Length Estimation in ±k Embedding Steganography,

Communications and Multimedia Security 2005.

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