A Systematic way to Design New Approach for Technical Steganography based on ACO Algorithm

Gurjeet Kaur*, Rupinder Kaur
Doaba institute of Engg. & Technology, Kharar
Gurjeetbjwa123@gmail.com*, rupinder8610@gmail.com

Abstract: Steganography is a talent of hiding statement by embedding message into an innocuous observing cover media. Using steganography, a Thankfully message is embedded inside a piece of unsuspicuous information. Image steganography is a technique of conceal information into a cover image to hide it. DWT based approach is widely accepted steganography methods in frequency domain due to its simplicity and hiding ability. A novel method for Image steganography based on Least Significant Bit using X-box mapping where we have used several wavelets having unique data. The embedding part is done by this Steganography algorithm where we use four unique bounds which has be consider in two parts i.e. lower bound and upper bound with values of the cover image. This wavelet provides adequate security to the load because with no significant the transformation rules no one can extract the secret data. Second Approach, we can implement the Ant Colony Optimization Technique for extract the message from the cover image or original image. After that we can classify the design system using Back Propagation Neural Network which has been creating in two modules like Training Module and other one Testing Module. Many information security algorithms have been developed steganography algorithms to enhance information security. One of the most recent algorithms is Neural Network. In this paper it encrypts the secret message to protect it from being accessed by unauthorized users before being hidden. The PSNR of the stego image was estimated to measure the stego images quality. The obtained results demonstrated that using secret key provides good security and PSNR value higher than previous image steganography methods. Similarly, DWT and ACO have been used to embedding and extraction process of secret message will be done using Transformation and optimization technique. So in the paper, Back Propagation Neural Network, DWT and ACO with lower Bound and Upper Bound will be introduced. Lastly, we design the secure system to hide the message in the image using testing module checked the performance parameters like Peak Signal to Noise Ratio, Mean Square Error and Root Signal Error. To compare the performance parameters with the previous approaches like (LSBand X-box mapping) on the basis of PSNR and MSE.

Keywords:  DWT, ACO, PSNR, MSE, BPNN, JPEG, Steganography

I. INTRODUCTION

The Information Security is gaining importance because of the use of data being transferred on the network. Hence, the data integrity and confidentiality are important aspects in the field of Network Security. Now days, the attackers have more computing power to be able to break encryption algorithms and these capabilities will only increase in the future. Here, “the importance of steganography lies as it hides the existence of the secret message which makes the job of attacker more difficult” Steganography, i.e. writing a piece of hidden message into a cover object to conceal its existence, has received much attention from the community. JPEG (Joint Photographic Experts Group) images are considered as practical covers for steganography because they are widely used and disseminated.

- The Cover image into which the secret message hides
- The Secret message which may be a plaintext, cipher text or any other type of data
- The Hiding Function or the key(along with the X-Box)
- The Stego image which is generated after the embedding of secret message into the cover image
- The Extract Function which will separate the secret message and the cover image

Figure 1: Basic Operation of Steganography

A. Different kinds of steganography

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object’s use and display [11]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [5]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

B. Image Steganography

Images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific...
applications. For these different image file formats, different steganographic algorithms exist. To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image [14]. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image’s pixels (represented as bits) where each pixel is located and its colour [15]. These pixels are displayed horizontally row by row. Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [2]. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image. Steganography in the transform domain involves the manipulation of algorithms and image transforms [17]. These methods hide messages in more significant areas of the cover image, making it more robust [4]. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression [18].

Figure 3: Categories of image steganography

C. Applications of Steganography

- **Secret Communications**: The use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.
- **Feature Tagging Elements** can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.
- **Copyright Protection**: Copy protection mechanisms that prevent data, usually digital data, from being copied. The insertion and analysis of water-marks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding.

II. RELATED WORK

It is believed that steganography was first practiced during the Golden Age in Greece. An ancient Greek record describes the practice of melting wax off wax tablets used for writing messages and then inscribing a message in the underlying wood. The reviews of different techniques are:

**BingwenFeng et al., 2014** [15] described as, a binary image steganography scheme that aims to minimalize the embedding distortion on the texture is presented. They extracted the complement, rotation, and mirroring-invariant local texture patterns from the binary image first. The weighted sum of crmltchanges when flipping one pixel is then employed to measure the spinning alteration corresponding to that pixel.

**Saiiful Islam et al., 2014** [17] proposed a novel steganography method, where edges in the cover image have been used to surround messages. Amount of data to be embedded plays a significant role on the selection of edges, i.e., the more the quantity of data to be embedded, larger the use of weddier edges for embedding.

**Rupesh Gupta et al., 2014**, [21] In this paper, planned and they worked but as the impostors are acting quickly to hack information developers are also imaginary to invent new techniques to stop hacker’s purposes. As per the basic information more is the PSNR value and lesser is the MSE consequences are better so, here in this paper they are suggesting a new method by combing three major security systems that is cryptography, steganography and watermarking that will not only hide the evidence but produce better consequences.

**Saravanan et al., 2013** [23] This paper decreases the obvious distortion in a joint photographic experts group file during data hiding process, by presenting new region selection rule. The new region selection rule reflects three factors, i.e., the horizontal difference, vertical difference and region size. The JPEG image will be split into quantity of blocks and each pixel in it will be inspected to calculate the differences. Depends upon the difference, the amount of secret material will be hide in an image.

III. RESEARCH PROBLEM

Steganography is a technique which leads to hiding content of one format to additional or within the same arrangement. In case of an image there has been a lot of work has been done in the same contrast. I can search a lot of papers and study then review the previous techniques and algorithms.

- The methods have been proved to a revolutionary step in the field of data hiding. As the passes on, the complexity to hide the data growths. They also need to prevent the base image (refers to the image in which we are hiding the data), so that if the image gets chopped the hacker won’t be able to assume that some data has been into the base image by looking at the image [25].
- To achieve the same, a lot of previous algorithms have been proposed like DWT, DCT and so many other procedures.
- In this paper, the problem statement involves use of seed values in such a way that the IMAGE QUALITY which is measured in terms of PSNR increases and the data remains safe within the image. The process goes on as; a sequence of random numbers is first generated by a pseudo-random number generator with an arbitrary seed.
- Then the cover image is divided into dynamic-size blocks using this sequence a route is created and the secret data is embedded into the LSB of the pixels.
along this route. Among the routes twisted by repeating this process with different seeds, the best route which produces minimal distortion is chosen for data embedding.

IV. RESEARCH OBJECTIVES

The research paper encompasses a set of objectives that is associated with milestone of this process. The research objectives are described as:

- To study the existing techniques for image steganography.
- To implement the frequency domain technique using Discrete Wavelet Transformation.
- To add text and apply Ant colony optimization algorithm for optimization of results.
- After optimization, to apply the BPNN algorithm for classification purpose.
- To analyze and compare the results with the previous approaches on the basis of performance parameters such as PSNR, Time and MSE.

V. PROPOSED METHODOLOGY

The following steps present the different stages that need to be accomplished:

- Upload the cover image (original Image).
- Apply the Frequency domain technique to divide the image in Lower bound and upper bound.
- To add the text in image for hiding (Security), after hiding we use the ant colony algorithm for reduction.
- Last one to classify the data in two sets like Training and Testing set.
- To evaluate the performance parameters like Peak signal to noise ratio and Mean square error.

A. Performance Metrics

1. PSNR: Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the determined possible power of a signal and the power of corrupting noise that affects the reliability of its representation.

   \[
   PSNR = 20 \log_{10} \left( \frac{MAX_f}{\sqrt{MSE}} \right)
   \]

2. MSE: In measurements, the mean squared error of an estimator is one of many ways to quantify the variance between values implied by an estimator and the true values of the quantity being estimated.

   \[
   MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \| f(i,j) - g(i,j) \|^2
   \]

3. Time Consumption: This parameter used to check efficiency of algorithm based on detection time of any information form a stego image. Because of the main part of process to find the content from the stego image so that the extraction time consumption parameter considered. Time consumption is in milli seconds for reconstruct the data bits and generate the original embedded message.

VI. SIMULATIONS RESULTS

Steganography (also known as "steg" or "stego") is "the art of writing in cipher, or in characters, which are not intelligible except to persons who have the key; cryptography". In computer terms, steganography has evolved into the practice of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. In contemporary terms, steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file (like a.wav or mp3) or even a video file.

- Like many security tools, steganography can be used for a variety of reasons, some good, some not so good.
- Legitimate purposes can include things like watermarking images for reasons such as copyright protection. Digital watermarks (also known as fingerprinting, significant especially in copyrighting material) are similar to steganography in that they are overlaid in files, which appear to be part of the original file and are thus not easily detectable by the average person.
- Steganography can also be used as a way to make a substitute for a one-way hash value (where you take a variable length input and create a static length output string to verify that no changes have been made to the original variable length input).
- Steganography can be used to tag notes to online images (like post-it notes attached to paper files).
- Steganography can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.
- Steganography can also be used for illegitimate reasons.
- If someone was trying to steal data, they could conceal it in another file or files and send it out in an innocent looking email or file transfer.

A. Implementation Results

![Figure 4. GUI of the Steganography using ACO](image)

Above figure clearly shows that the central page processing means upload the image from the dataset and find the wavelet in the image (lower bound and upper bound), after that, apply the ant colony optimization and then classification techniques using BPNN.
Above figure shows that, consequences find the optimize values and best solution. We achieved the 1*200 matrix original data. After ACO algorithm 1*100 reduce the wavelet values.

In above figure, apply the discrete wavelet transformation for image convert into four bonds, but wavelet convert the only 2 bound (upper and lower) according to the maximum and minimum values of the wavelets.
Figure 12: Convert the message in binary format (stego image)

Above figure defines, an embed the message in image, and then change the original format to binary code. Because of the second client can’t read the message you can embed the image. This is used for security purpose. Figure described the message embed the image and generate the stego image.

Figure 13: outcomes of the performance Parameters

Above figure, defines the performance parameters like mean square error, peak signal to noise ratio, root mean square error and time consumption.

B. Output Tables

The output table shows the results on the basis of performance parameters for different images after applying the steganography using ACO.

Table1: Outcomes on the basis of Performance Parameters for Steganography using ACO

<table>
<thead>
<tr>
<th>Image no.</th>
<th>Mean error (MF)</th>
<th>Square Peak Signal to noise ratio</th>
<th>Time Consumption (msec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.15406</td>
<td>85.288</td>
<td>0.04842</td>
<td></td>
</tr>
<tr>
<td>0.10865</td>
<td>65.184</td>
<td>0.0021732</td>
<td></td>
</tr>
<tr>
<td>0.10447</td>
<td>67.9749</td>
<td>0.0021516</td>
<td></td>
</tr>
<tr>
<td>0.11572</td>
<td>68.5307</td>
<td>0.0027006</td>
<td></td>
</tr>
</tbody>
</table>

Table2: Comparison between previous and proposed work

<table>
<thead>
<tr>
<th>Image no.</th>
<th>Mean Square Error (ME)</th>
<th>Mean Square Error (ME)</th>
<th>Peak Signal To Noise Ratio (PSNR)</th>
<th>Peak Signal To Noise Ratio (PSNR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.13174</td>
<td>0.15406</td>
<td>50.9881</td>
<td>65.288</td>
<td></td>
</tr>
<tr>
<td>0.34574</td>
<td>0.10865</td>
<td>39.6552</td>
<td>85.184</td>
<td></td>
</tr>
<tr>
<td>0.049877</td>
<td>0.10447</td>
<td>42.1054</td>
<td>87.9749</td>
<td></td>
</tr>
</tbody>
</table>

VII. CONCLUSION & FUTURE WORK

Steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. Although related, Steganography is not to be confused with Encryption, which is the process of making a message unintelligible—Steganography attempts to hide the existence of communication. Steganography is an effective way to hide sensitive information. The objective of this research was to enhance steganography in digital images. The proposed system has discussed implementation of securely using steganography technique based on BPNN, ACO and DWT algorithm. It can be concluded that when normal image security using steganography technique is applied, it makes the task of the investigators unfeasible to decrypt the encoded secret message. The security features of the steganography are highly optimized using seed values algorithm. Image Steganography has many applications, especially in today’s modern, high-tech world. Privacy and anonymity is a concern for most people on the internet. Image Steganography allows for two parties to communicate secretly and covertly. It allows for some morally-conscious people to safely whistle blow on internal actions; it allows for copyright protection on digital files using the message as a digital watermark.

FUTURE WORK

In the future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate. We can also applied proposed technique to computer forensic images. So that the system can generate highly undetectable secret shares using encryption techniques certain set of training data which might be automatically generated and is disposed after the task has been performed.

REFERENCES


