Level's 4 Security in Image Steganography

Harpreet Kaur
University College of Engineering, Punjabi University, Patiala
Patiala, Punjab, India

Gaurav Deep
University College of Engineering, Punjabi University, Patiala
Patiala, Punjab, India

ABSTRACT
Steganography means secret writing of hide data in any others from of digital media . It may be Video,Audio, Text, Image, etc Data security is the requirement of digital media. Digital media to make it secure over a various techniques/Methods have been proposed by many researchers over decades.. To take step further we propose a new method in steganography .Which use RGB model in Image steganography. The proposed methodology is a combination of three techniques, Graph partitioning, clustering and pattern matching. These three techniques are used collectively to introduce a new technique which can be used in steganography, provide upper level of security and increase data hide capacity.

Keywords
RGB Image, RGB Color Model, Steganography, Graph partitioning, Clustering, Level's 4 security.

1. INTRODUCTION
Steganography can be defined as the art and science of hiding data so that no one knows about hidden data except the sender and receiver. This is not a new concept , a new era of this technique has started as computer came into existence as different algorithms are used to hide data with different cover media[1].

1.1 General specification of Steganography
In today's modern world, there are large number of methods that are used to implement steganography but the general description that is used in each Implementation is follows[2] .

Hidden Data: The data that is to be sent it must not be known to unauthorised user over the network.

Cover media*:* Cover media can be an image an audio video file. The media in which secret data is to be hidden.

Stego-key*:* This key is used to provide security by implementing cryptography. This technique is useful in a way such that even if hidden data is found, than it will not be in human understandable form but in a scrambled form, hence provides additional security.

Stego-media: It contain to hide data and that file sent over the channel to the intended recipient.

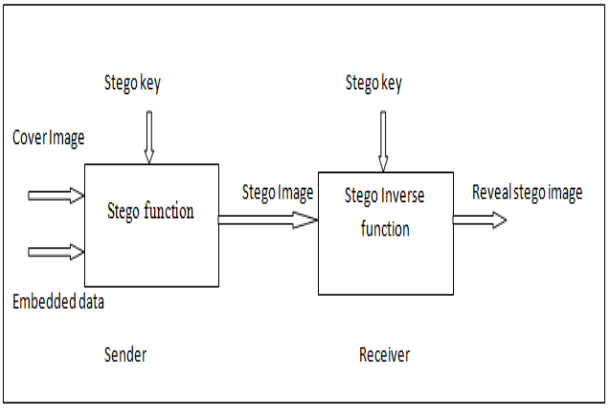

Figure 1 Concept used for Steganography

1.2 Types of Steganography
Steganography is the science of invisible communication. Steganography is used for secret writing so that intruders can not find hidden data.This communication takes place by hiding data .There are various techniques used in steganography are as follows:

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Network Steganography

1.3 Characteristics of Steganography:
1. Confidentiality.
2. Imperceptibility.
3. Accurateness.
4. High capacity.
5. Resistance.
6. Visibility
7. Survivability

1.4 Goals of Steganography
The goal of Steganography is to hide the data from third party whereas the goal of cryptography is to make data unreadable by third party. Steganography is used to hide data over cover media. There aresome various features of steganography are:

1. The data must Remain hidden that is main goal of steganography.
2. The data should be hidden in such a way that even if it is viewed by user, than it must not gain any focus

from viewer's eye, therefore the data is in visible form but still cannot be recognized.

3. It provided better imperceptibility.
4. The secret data should be directly hidden into the cover media it can be image, audio or video rather than into a header or wrapper , to maintain data consistency.
5. The quality of the cover media should not be degraded by embedding the secret data and the embedded data should be imperceptible as much as possible.

2. IMAGE STEGANOGRAPHY

It is the most widely used technique for secret communication.Human eye cannot detect the variation in luminance of color vectors at high frequency side of the visual spectrum. This technique exploits the limitations of Human Visual System. The individual pixels can be represented by their optical characteristics like brightness,chrominance etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s. A picture is a represented by a collection of color pixels Different images are used for image steganography with different methods to hide information, each having its own advantage and limitation[2]. For example: a 24-bit bitmap have 8 bits, representing each of the three color values red, green, and blue at each pixel [3].The approach for embedding information in cover image is using Nearest Neighbourhood pixel technique . This is a simplest steganography technique embed the bits of the message directly into their neighbourhood pixels of the cover image .So that hackers/attackers are very difficult to find the exact pixel location where the message is actually hide.

When message is converted into bit format, than the nearest neighbourhood pixel of that particular pixel is actually used for hide our secret message., we must insert a small amount of data in a pixel to expand hidden message in image. This task can be accomplished with the help of Nearest Neighbourhood pixel technique in particular pixel to hide data. Message size should be of small size as compared to size of cover media.

3. RGB MODEL BASED IMAGE STEGANOGRAPHY

3.1 RGB

It is used for display Image on electronics system like Computer monitors and televisions are the most common examples of additive color. RGB is additive color model. Each RGB color model contain 8 bit for Red, Green and Blue clolor. Digital images are typically stored in either 24-bit (RGB) or 8- bit (Grayscale) files. A 24-bit image provides the most space for hiding information; however it can be quite large (with the exception of JPEG images). RGB color model basically used for the representation,display and sensing, of images in electronic systems, such as computers ,televisions and, conventional photography.RGB color model are used for data insertion and extraction in Steganography.

3.2 Advantages of RGB color model

The RGB intensity based steganography technique consists of following advantages:

- This technique is provided more security for hiding data because third party cannot easily detect the presence of hidden data.
- RGB is simplest and the most common model.
- Embeds large amount of data as compared to previous techniques one of the main advantages is its capacity.

4. GRAPH PARTITION

Graph partitioning is defined on data represented in the form of a graph $g = (v,e)$, with e edges and v vertices , such that it is possible to partition g into smaller components with specific properties.. For instance, a k-way partition divides the vertex set into k smaller components. A good partition is defined as one in which the number of edges running between separated components is small There is uniform graph partition is a type of graph partitioning problem that consists of dividing a graph into components. Such that the components are of about the same size and there are few connections between the components. These are the important applications of graph partitioning are partitioning various stages of a VLSI design circuit and task scheduling in multi-processor systems .. [16]

4.1 Graph partitioning properties

- Data should be consistent.
- Unauthorised users does not access partitioning block data over the image.
- Graph partitioning is better way for hiding data.

5. CLUSTERING

Clustering is the process of organizing the objects in such a way that objects within the cluster are similar to each other and dissimilar to other objects.The process of creating clusters is known as clustering. The purpose of clustering is get meaningful result,Clusters can be created according to color, size etc. Effective use of storage and fast retrieval in various area. This approach is also used image steganography.[1].

6. METHODOLOGY

A. At Sender side: The main steps that are required to hide data by using this technique are as follows:

Input Image: Select a color image as cover media.

Graph Partitionng*:* Apply Graph Partitioning on color Image which creates multiple partitioned blocks in cover image.

Clustering**:** Create clusters in randomly selected block based on color feature by using RGB color model.

Selection of Cluster: In Graph Partitioning block to hide data select largest cluster.

Apply Steganography: Hide data using private key steganography.

Stego- image: Generate Stego- image**.**

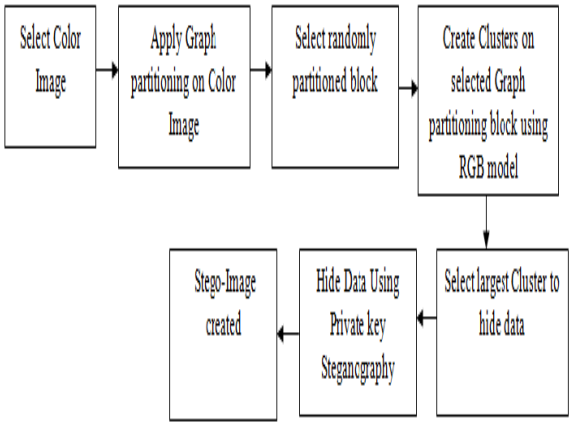

Fig .2 A general mechanism of generating stego-image from input Image

At Receiver side: At receiver side the procedure is applied in inverse form which is as follows:

***Input Stego-Image*:** Take the stego-image as input.

***Private Key**:* Receiver generate Private key for decrypt data

Graph partitioning*:* Apply graph partitioning on stego image to create multiple partitioned blocks.

***Clustering*:** Create clusters in selected partitioned block according to color feature by using RGB color model.

***Identify Cluster*:** Identify the largest cluster in which information is hidden.

***Extraction*:** Extract the hidden data.

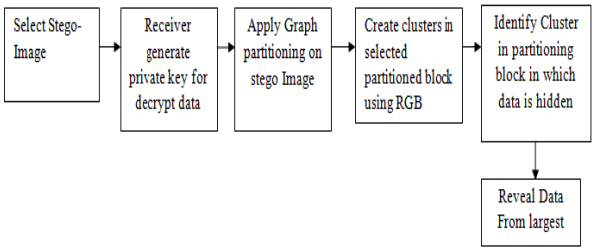

Fig. 3: A general mechanism of generating hidden data from Stego-Image.

7. PROPOSED WORK

We have proposed a new technique of hiding data in algorithm by graph partitioning on color Image: apply graph partitioning on input color image, select particular graph partitioned block and create clusters based on the RGB color model, select largest cluster among three RGB clusters to store maximum amount of data, and then hide data using nearest neighbour steganography. There are various techniques used for hiding data in steganography Four level of security is achieved as in level1 there is input cover Image, level 2 contains particular partitioned block, level 3 creating clusters in random partitioned block and level 4 contains largest cluster to embed data, using 4 level's security data become more secure from the previous steganography techniques. For achieving this objective we have used an algorithm which is Progressive Exponential Clustering(PEC) for creating clusters and calculating the size of clusters into random partitioned block on a digital Image. Progressive Exponential Clustering (PEC) aiming at striking a good balance between high embedding capacity and low embedding distortion.

Fig.4 Four Level's Security

8. IMPLEMENTATION

1. Choose color Image as cover media.
2. Multiple partitioned blocked of particular color Image is generates when we Apply graph partitioning algorithm.
3. After that PEC algorithm is applied in a randomly selected block.
4. Select largest cluster to hide data by using nearest neighbor steganography.
5. Stego-image is created which looks same as the original Image.

The general principle of this algorithm is as below:

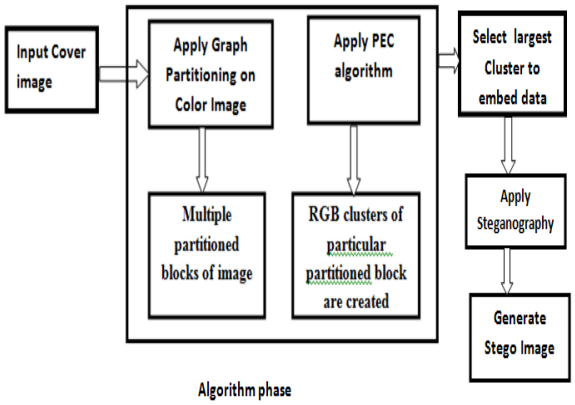

Fig. 4 General principle of proposed algorithm

9. RESULT

Figure 5. An image on which proposed technique is applied

Figure 6. After implementing proposed technique the stego-image generated

10. CONCLUSION

Various techniques for image steganography are discussed for example, spatial domain techniques such as LSB substitution which modify pixel value and Transform Domain Techniques such as DCT, Wavelet transform etc. It transform the spatial domain into frequency domain and applies steganography during quantization phase. In this technique, first of all, a input color image is selected, apply graph partitioning process on color image, Select particular partitioned block for pattern matching. In the particular partitioning block the clusters are created based on colored feature by using RGB color model, a color pattern (RGB) is generated along with clusters. These different clusters like (RGB) contain different number of pixels in the different partitioning blocks. The partitioning block having big cluster with largest number of pixels is selected to embed data. The stego-image generated When the embedding is completed,. Data and cannot be easily detected by the hacker/attacker.It also improves security with the help of partitioning blocks to hde data.This technique enhances the security in a better way as it provides four levels of security and also processing time is improved.

11. FUTURE SCOPE

In future, this technique can be used in a more advanced way such that In the different image graph partitioning block an image contains a number of clusters . Therefore, multiple messages can be embedded into the multiple clusters, such that each cluster in each partitioning block contains a particular message. Multiple messages can be sent in one cover file. All the color clusters can be used to hide data as we have used one cluster to hide data. This selection could be on increasing or decreasing order. Multiple image partitioning blocks can be used for hiding purpose as we have used one partitioning block to hide data. To enhance security cryptography can also be used. But message size must be in the limit according to cluster size such that it should not degrade the image quality**.**This technique can also be used on high quality images.

12. REFERENCES

[1] Chamkor singh, Gaurav Deep, "Cluster Based Image Steganography Using Pattern Matching", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 4, July – August *2013.*

[2] Deborah A. Whitiak, "The Art of Steganography".

[3] Shawn D. Dickman," An Overview of Steganography", JMUINFOSEC-TR-2007-002.

[4] Sanjeev Kumar and Jagvinder Kaur "Study and Analysis of Various Image SteganographyTechniques", IJCST Vol. 2, Issue 3, September 2011, ISSN: 2229 - 433

[5] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav," Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering.

[6] Arvind Kumar and Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9–No.7, November 2010