Cluster based Image Steganography using Pattern Matching

Chamkor Singh[#1], Gaurav Deep[*2]

[#]*University College of Engineering, Punjabi University, Patiala*
Sirsa, Haryana, India
[1]sran.chamkaur@gmail.com

[*]*University College of Engineering, Punjabi University, Patiala*
Patiala, Punjab, India
[2]deepgaurav48@gmail.com

Abstract—**"Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text).In this paper,a new methodology is presented to hide data in which image is used as cover media.The proposed methodology is a combination of two techniques, color clustering and pattern matching. These two techniques are used collectively to introduce a new technique which can be used in steganography.**

Keywords—**Steganography,Clustering,Pattern Matching.**

I. INTRODUCTION

With the expansion of the Internet, one of the most important factors of information technology was to secure the information. Cryptography was developed as a technique to hide the meaning of message. Various methods have been developed to encrypt and decrypt the message in order to hide its meaning. But sometimes it is not enough to hide the meaning of a message, it may also be necessary to hide the existence of message .This technique used to hide the message is known as Steganography[1].

To achieve steganography, following is required:

- Cover media that can be used to hide data. In this case, image is used as cover media.
- The secret data which is to be hidden.
- An algorithm which can be used to insert secret data in cover media.Its reverse algorithm is required on receiver side.
- A secret key can be used to secure data.

Steganography is the science of invisible communication .This communication takes place by hiding data inside data.The various techniques used in steganography are as follows:

- Text Steganography.
- Image Steganography.
- Audio Steganography.
- Video Steganography.
- Network Steganography.

A. Image Steganography

It is the most widely used technique for secret communication. This technique exploits the limitations of Human Visual System. Human eye cannot detect the variation in luminance of color vectors at high frequency side of the visual spectrum. A picture is represented by a collection of color pixels. 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. For example: a 24-bit bitmap will have 8 bits, representing each of the three color values (red, green, and blue) at each pixel[1].Different images are used for image steganography with different methods to hide information, each having its own advantage and limitation[4].

When message is converted into bit format, than its bits can be replaced with pixel value as a whole. But to expand hidden message in image,we must insert a small amount of data in a pixel. This task can be accomplished with the help of LSB modification in each byte.But it requires that message size should be of small size as compared to size of cover media.

II.CLUSTER BASED IMAGE STEGANOGRAPHY USING PATTERN MATCHING

A. Clustering

Clusters are the groups of similar objects(pixels).The objects are such that they are similar to each other in a cluster and dissimilar with objects of other clusters.The process of creating clusters is known as clustering. Clusters can be created according to color,size etc. One of the important thing is that the clusters always contain useful

information.Clustering on image helps to get different sets of useful data.This approach is also used in image steganography.

B. Pattern Matching using Color

A cluster is created with the help of pattern matching using color. The objects which are similar in color are collected in a cluster. In pattern matching, a color palette is used for comparison of color with pixel color[3].

To achieve steganography, color image is chosen as the cover media. The hidden message to be sent will be first embedded in image file before sending. In this technique, image is pre-processed before embedding message. The image is first divided into clusters. These clusters are created using pattern matching based on predefined color palette range.

After the clustering is applied over the image, a cluster is selected in which the secret message is to be embedded. After that, message is embedded in the cluster using steganography technique and an image is created by placing clusters at their proper positions. This stego-image is than sent over the channel.

On the receiver side, inverse procedure is applied. The stego-image is selected as input. Pattern matching is applied on the image for clustering. After the clusters have created, the cluster is identified in which the message is embedded. The message bits are extracted from the cluster and combined in meaningful and readable form.

III. METHODOLOGY

A. At Sender side:

The main steps that are required to hide data by using this technique are as follows:

1) *Input Image*: Select a color image to be used as a cover media.
2) *Pattern Matching*: Scan image according to basic colors by using pattern matching.
3) *Clustering*: Create cluster (using pattern matching) based on color feature.
4) *Selection of Cluster*: Select cluster in which the secret data is to be hidden.
5) *Apply Steganography*: Hide data in the color image.
6) *Send Image*: Send the stego-image over the channel.

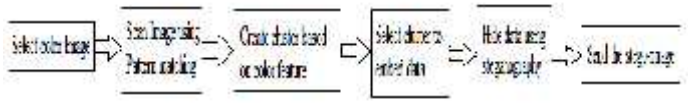

Fig. 1 Cluster based Image Steganography using Pattern Matching

B. At Receiver side:

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

1) *Input Stego-Image*: Take the stego-image as input.
2) *Pattern Matching*: Scan image by using pattern matching.
3) *Clustering*: Create cluster according to color.
4) *Identify Cluster*: Identify the cluster in which information is hidden.
5) *Extraction*: Extract the hidden data.

IV. FACILITIES REQUIRED

The facilities which are required in this methodology are as follows:

- The study of pattern matching techniques which are applicable on color image.
- To study various cluster algorithms and selection of a suitable cluster algorithm which will be used in image clustering using pattern matching.
- To study various pattern matching algorithms.
- To learn Matlab software in which this methodology will be coded.

V. CONCLUSION

In simple techniques, pixel value was directly replaced by secret data which was easy to retrieve. It was easy for the intruder or third party to extract the message bits and combine them to create a useful form. But this technique is not dependant on a single technique, it is a combination of more than one techniques and therefore it is not easy for the intruder to get the secret data. It imposes more protection on secret data. This technique can be more useful if it used in combination with cryptography so that if any intruder comes to know about the hidden data, than he cannot get that data in readable form. Therefore, it can prove to be more useful as it provides more security to confidential information.

REFERENCES

[1]Soumyendu Das, Shubhendu Das, Bijoy Bandhyopadhyay and Sugata Sanyal, "Steganography and Steganalysis:Different Approaches".

[2]Mrs. Kavita, Kavita Kadam, Ashwini Koshti and Priya Dhunghav," Steganography using Least Significant Bit Algorithm", *International Journal of Engineering Research and Applications(IJERA)*, Vol.2, Issue 3, May-Jun 2012.

[3]Kavin Curran, Karen Bailey," An Evolution of Image Based Steganography Methods", *International Journal of Digital Evidance*, Fall 2003, Volume 2, Issue 2.

[4]T. Morkal, J.H.P Eloff, M.S. Olivier,"AN OVERVIEW OF IMAGE STEGANOGRAPHY".

[5]P.Scheunders,"A COMPARISON OF CLUSTERING ALGORITHMS APPLIED TO COLOR IMAGE QUANTIZATION".

[6]http://zone.ni.com/reference/en-XX/help/372916j-01/nvisionconcepts/color_pattern_matching

[7]R.C. Gonzalez and R.E. Woods,"Digital Image Processing",2nd Edition,2002.

[8]S.Annadurai and R.Shanmugalakshmi,"Fundamentals of Digital Image Processing",Pearson.